

Computer Forensics: Technology, Policy and Countermeasures

Simson L. Garfinkel, Ph.D.
<http://www.simson.net/>

June 17, 2007
Usenix 2007 General Conference
Santa Clara, CA

A bit about me

Tech Journalist: 1985—2002

Entrepreneur: 1988—2002

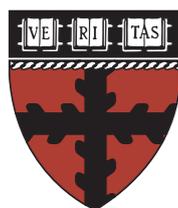
Vineyard.NET, Broadband2Wireless,
Sandstorm Enterprises, Inc.

MIT EECS 2002—2005

Fellow, 2005—

Center for Research on Computation and Society,
School of Engineering and Applied Sciences,
Harvard University

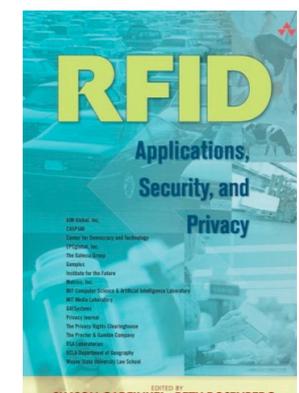
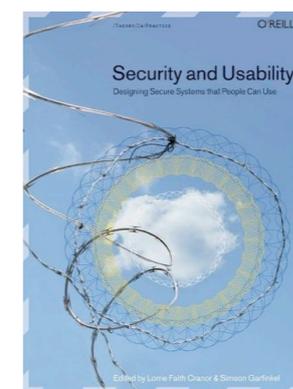
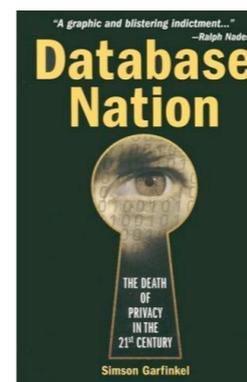
Associate Professor, 2006—
Naval Postgraduate School,



Harvard
School of Engineering
and Applied Sciences

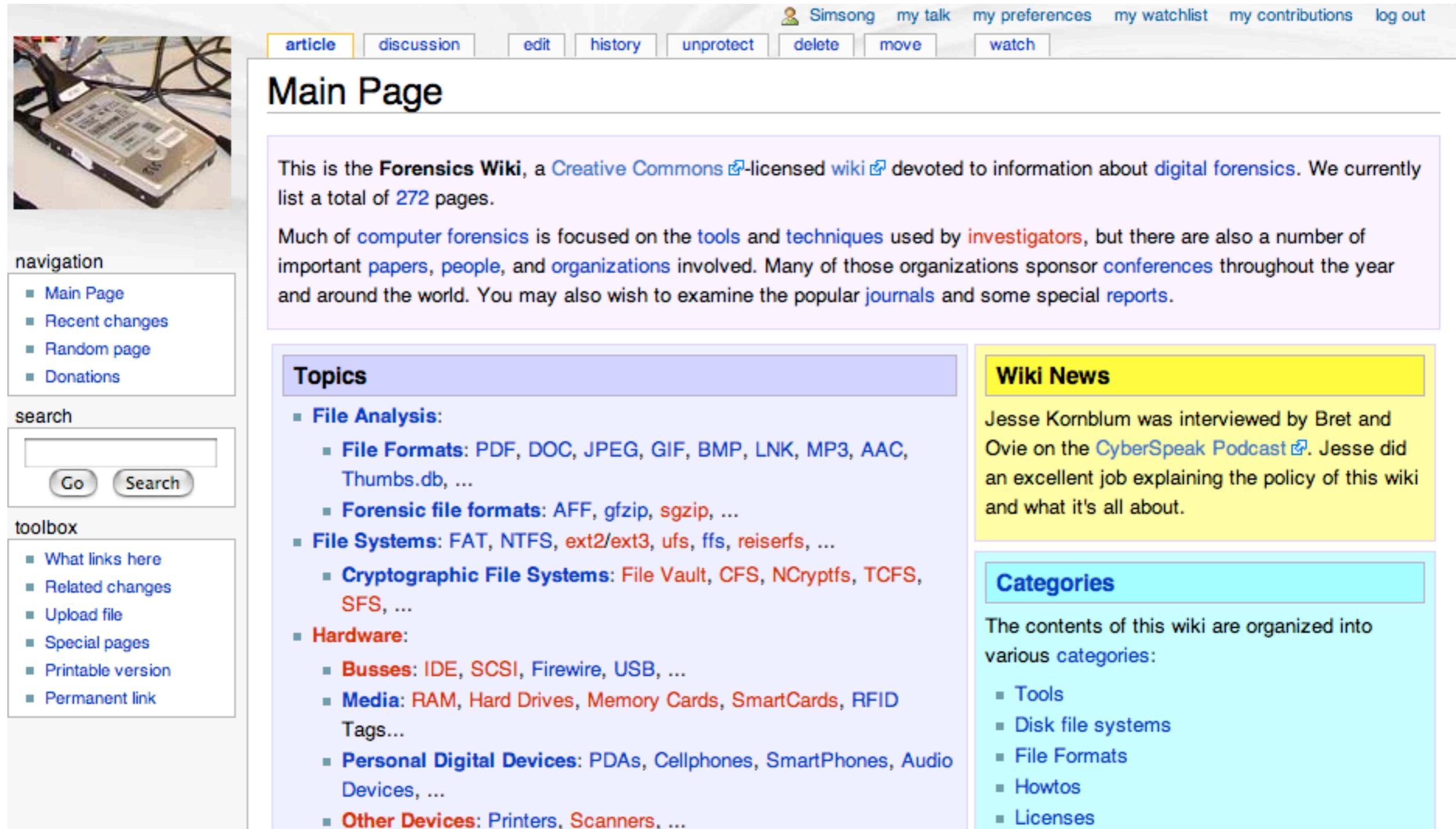


“Used Hard Drives
Reveal Secrets.”



I maintain the Forensics Wiki.

<http://www.forensicswiki.org/>



The screenshot shows the Main Page of the Forensics Wiki. At the top right, there is a user profile for 'Simsong' with links for 'my talk', 'my preferences', 'my watchlist', 'my contributions', and 'log out'. Below this is a navigation bar with buttons for 'article', 'discussion', 'edit', 'history', 'unprotect', 'delete', 'move', and 'watch'. The main heading is 'Main Page'. The introductory text states: 'This is the **Forensics Wiki**, a [Creative Commons](#)-licensed [wiki](#) devoted to information about [digital forensics](#). We currently list a total of [272](#) pages.' It continues: 'Much of [computer forensics](#) is focused on the [tools](#) and [techniques](#) used by [investigators](#), but there are also a number of important [papers](#), [people](#), and [organizations](#) involved. Many of those organizations sponsor [conferences](#) throughout the year and around the world. You may also wish to examine the popular [journals](#) and some special [reports](#).' The page is divided into three main sections: 'Topics', 'Wiki News', and 'Categories'. The 'Topics' section lists: 'File Analysis' (with sub-items: File Formats: PDF, DOC, JPEG, GIF, BMP, LNK, MP3, AAC, Thumbs.db, ...; Forensic file formats: AFF, gzzip, sgzip, ...); 'File Systems' (with sub-items: Cryptographic File Systems: File Vault, CFS, NCryptfs, TCFS, SFS, ...); and 'Hardware' (with sub-items: Busses: IDE, SCSI, Firewire, USB, ...; Media: RAM, Hard Drives, Memory Cards, SmartCards, RFID Tags...; Personal Digital Devices: PDAs, Cellphones, SmartPhones, Audio Devices, ...; Other Devices: Printers, Scanners, ...). The 'Wiki News' section features a yellow background and a news item: 'Jesse Kornblum was interviewed by Bret and Ovie on the [CyberSpeak Podcast](#). Jesse did an excellent job explaining the policy of this wiki and what it's all about.' The 'Categories' section has a light blue background and states: 'The contents of this wiki are organized into various categories:' followed by a list: Tools, Disk file systems, File Formats, Howtos, Licenses. On the left side, there is a sidebar with a navigation menu (Main Page, Recent changes, Random page, Donations), a search box with 'Go' and 'Search' buttons, and a toolbox menu (What links here, Related changes, Upload file, Special pages, Printable version, Permanent link). At the top left of the main content area, there is a small image of a hard drive.

This tutorial looks at the range of forensic techniques currently in use

1. Introduction: What is Forensics?

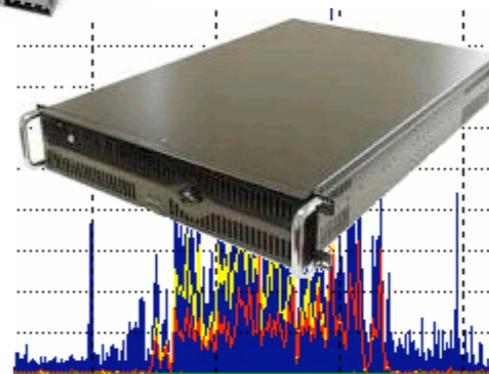
2. The Forensic Process

3. Legal Standards

4. Specific Forensic Techniques

- Disk Forensics
- Network Forensics
- Document Forensics
- Memory Forensics
- Cell Phone Forensics
- Software Forensics

5. Anti-Forensics



```
printf("%d, %f", i, f);  
    i++; f+=3.0;  
    g = fmod(f,i);
```

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

(b) When UN inspectors departed Iraq, the placement of HUMINT agents and the development of unaffiliated 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.

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 was hard to maintain... it takes a rare officer who can go in... and survive scrutiny... for a long time." The Committee agrees that such operations are difficult and dangerous, but they should be within the scope of the CIA's activities and capabilities. Some CIA officials have repeatedly told the Committee that a significant increase in funding and personnel will be required to enable the CIA to possess sufficient HUMINT assets similar to those of the Intelligence Community, 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.

(b) 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 -

CDROM #1: “Forensic Tools”



Disk images for analysis and carving:

- 11-carve-fat — FAT file system for carving
- 12-carve-ext2 — EXT2FS file system for carving
- 2-kwsrch-fat
- 8-jpeg-search

Tools:

- lucas_cygwin.pdf - Instructions for running SleuthKit and Autopsy under Windows with Cygwin
- NIDemo3.2 - Sandstorm Enterprises NetIntercept Demo
- WireShark - Packet interception tool (“ethereal”) for Windows & Unix
- autopsy-2.08.tar.gz — Autopsy source code

Documents: NIST standards, Search & Seizure manual & “Diversity Analysis”

CDROM #2: Helix 1.8 Discovery & Response

Dual-mode CDROM

Boot for “Live CD”:

- Linux system which treats PC in “forensically sound manner.” (doesn’t swap, mounts disks r/o, etc.)
- Many analysis tools, all precompiled
- Tools for both Windows and Unix

Insert and run for Live Analysis under Windows

- Inspect memory, live file system, etc.
- Great for systems that are password-protected, encrypted, etc.



Plan for today

Work through the slides

Break for food as necessary

Use “spare time” to look at tools on CDROMs.

Take lots of questions.



http://commons.wikimedia.org/wiki/Image:Wall_clock.jpg

Plan for today

Work through the slides

Break for food as necessary

Use “spare time” to look at tools on CDROMs.

Take lots of questions.



http://commons.wikimedia.org/wiki/Image:Wall_clock.jpg

Questions?

“Forensics:” Two Meanings

fo·ren·sics n. (used with a sing. verb)

- 1.The art or study of formal debate; argumentation.
- 2.The use of science and technology to investigate and establish facts in criminal or civil courts of law.

(American Heritage Dictionary, 4th Edition)



“Computer Forensics:” At least two meanings.



1. “Involves the preservation, identification, extraction, documentation, and interpretation of **computer data**.”
(*Computer Forensics: Incident Response Essentials*, Warren Kruse and Jay Heiser.)
2. “The scientific examination, analysis, and/or evaluation of **digital evidence** in legal matters.”
(*Scientific Working Group on Digital Evidence*, <http://www.swgde.org>)

But what's Digital Evidence?

“Information stored or transmitted in binary form that may be relied upon in court” [Int02]

“Information of probative value that is stored or transmitted in binary form” [Sci05]

“Information and data of investigative value that is stored on or transmitted by a computer” [Ass05]

“Any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi” [Cas04]

Evidence means that this information is used in a **legal process** (e.g. employee termination, lawsuit, court case, etc.)

Evidence is typically collected *after* criminal activity is suspected.

Crimes against computers:

- Break-ins; denial-of-service attacks.

Crimes involving computers:

- Distribution of child pornography; emailed threats

Computer forensics allows investigators to:

- Discover how a crime was committed
- Determine extent of damage
- Gather evidence of illegal activity
- Confirm/disprove an alibi



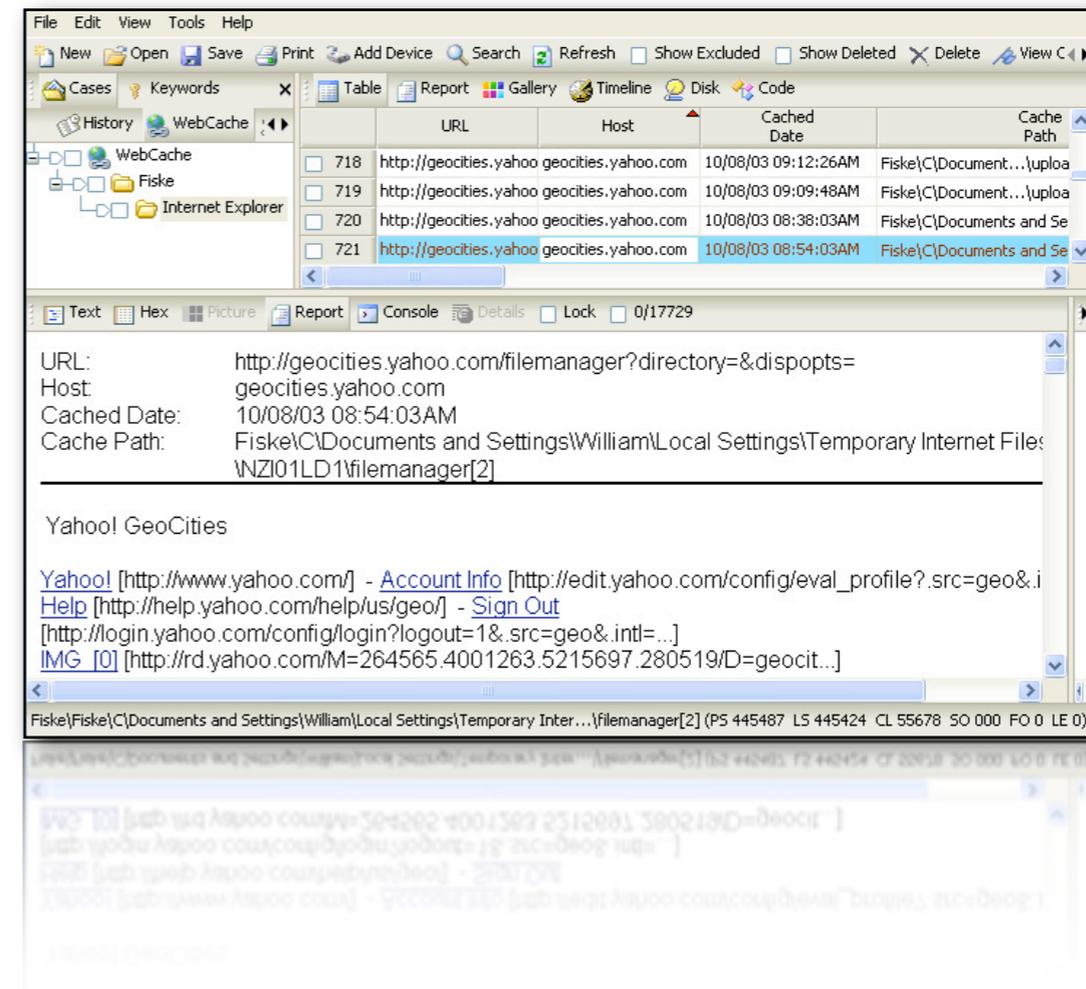
Computer Forensics is like a magic camera

Tools can go “back in time...”

- View previous versions of files
- Recover “deleted” files
- Find out what was typed
- Discover visited websites

Why does this work?

- Computers keep extensive logs
- Most data is not encrypted
- free() doesn't erase memory
- DELETE doesn't erase files
- FORMAT doesn't wipe disks



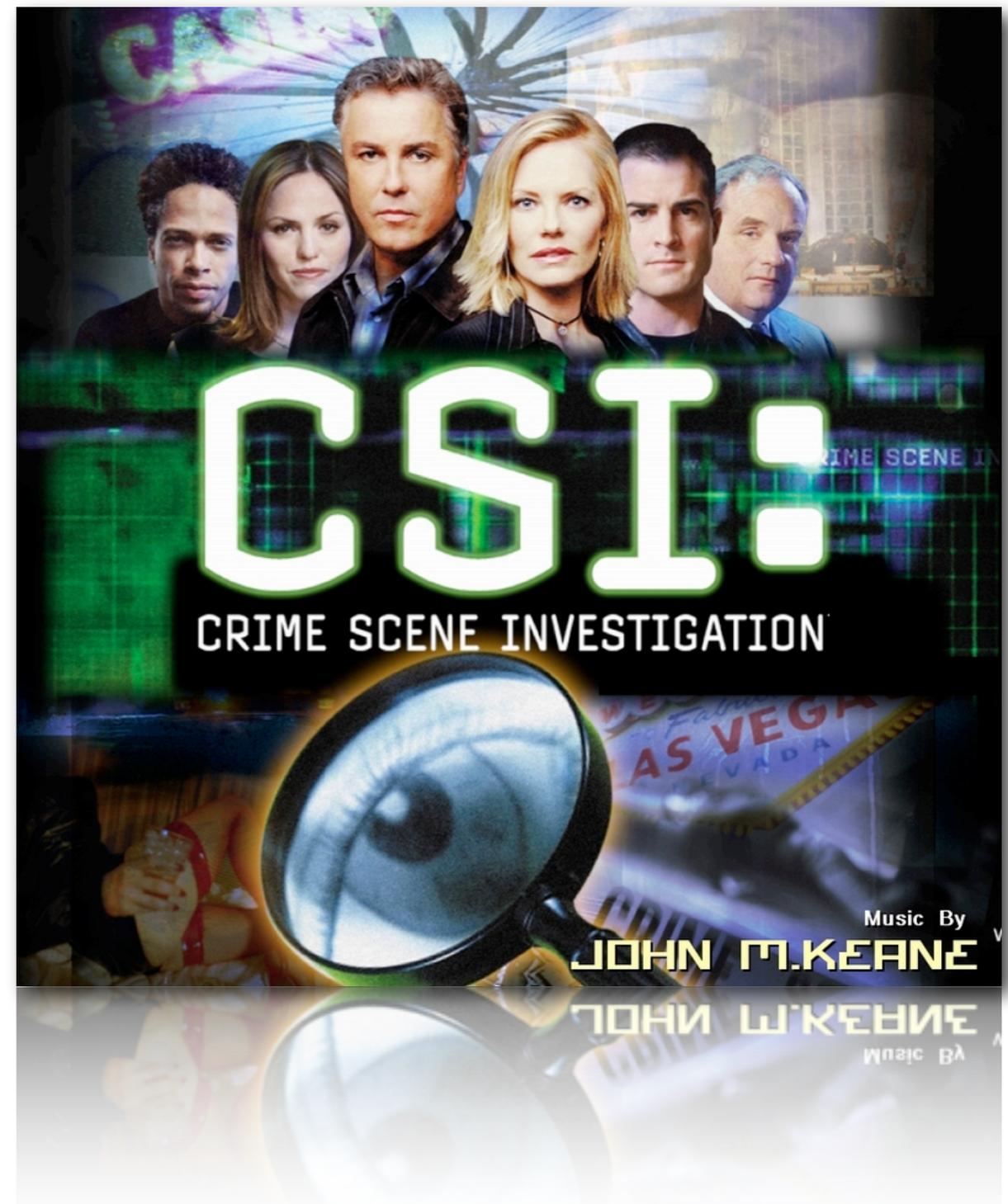
Unfortunately, the “CSI Effect” causes victims and juries to have unrealistic expectations.

TV shows fiction:

- Forensics are *swift*
- Forensics are *certain*
- Human memory as reliable
- Presentations highly produced

With computer forensics:

- Impossible to delete anything.
- Tools reliable
- Every investigator trained on everything.



A fundamental problem with computer evidence:
It can't be trusted.

A fundamental problem with computer evidence:
It can't be trusted.

Consider this printout:

A fundamental problem with computer evidence: It can't be trusted.

Consider this printout:

```
07:16 AM Black:~/slg/papers/afyi$ ls -l afyi.tex
```

A fundamental problem with computer evidence: It can't be trusted.

Consider this printout:

```
07:16 AM Black:~/slg/papers/afyi$ ls -l afyi.tex
-rw-r--r--  1 simsong  simsong  73625 Jun 16 07:15 afyi.tex
```

A fundamental problem with computer evidence: It can't be trusted.

Consider this printout:

```
07:16 AM Black:~/slg/papers/afyi$ ls -l afyi.tex
-rw-r--r--  1 simsong  simsong  73625 Jun 16 07:15 afyi.tex
08:13 AM Black:~/slg/papers/afyi$
```

A fundamental problem with computer evidence: It can't be trusted.

Consider this printout:

```
07:16 AM Black:~/slg/papers/afyi$ ls -l afyi.tex
-rw-r--r--  1 simsong  simsong  73625 Jun 16 07:15 afyi.tex
08:13 AM Black:~/slg/papers/afyi$
```

Question: Was `afyi.tex` modified 1 minute before the file was listed?

A fundamental problem with computer evidence: It can't be trusted.

Consider this printout:

```
07:16 AM Black:~/slg/papers/afyi$ ls -l afyi.tex
-rw-r--r--  1 simsong  simsong  73625 Jun 16 07:15 afyi.tex
08:13 AM Black:~/slg/papers/afyi$
```

Question: Was `afyi.tex` modified 1 minute before the file was listed?

Alternative explanations:

A fundamental problem with computer evidence: It can't be trusted.

Consider this printout:

```
07:16 AM Black:~/slg/papers/afyi$ ls -l afyi.tex
-rw-r--r--  1 simsong  simsong  73625 Jun 16 07:15 afyi.tex
08:13 AM Black:~/slg/papers/afyi$
```

Question: Was `afyi.tex` modified 1 minute before the file was listed?

Alternative explanations:

- The file was listed 57 minutes later.

A fundamental problem with computer evidence: It can't be trusted.

Consider this printout:

```
07:16 AM Black:~/slg/papers/afyi$ ls -l afyi.tex
-rw-r--r--  1 simsong  simsong  73625 Jun 16 07:15 afyi.tex
08:13 AM Black:~/slg/papers/afyi$
```

Question: Was `afyi.tex` modified 1 minute before the file was listed?

Alternative explanations:

- The file was listed 57 minutes later.
- The file was modified on a different day

A fundamental problem with computer evidence: It can't be trusted.

Consider this printout:

```
07:16 AM Black:~/slg/papers/afyi$ ls -l afyi.tex
-rw-r--r--  1 simsong  simsong  73625 Jun 16 07:15 afyi.tex
08:13 AM Black:~/slg/papers/afyi$
```

Question: Was `afyi.tex` modified 1 minute before the file was listed?

Alternative explanations:

- The file was listed 57 minutes later.
- The file was modified on a different day
- The computer's clock was changed before the file was modified and/or listed.

A fundamental problem with computer evidence: It can't be trusted.

Consider this printout:

```
07:16 AM Black:~/slg/papers/afyi$ ls -l afyi.tex
-rw-r--r--  1 simsong  simsong  73625 Jun 16 07:15 afyi.tex
08:13 AM Black:~/slg/papers/afyi$
```

Question: Was `afyi.tex` modified 1 minute before the file was listed?

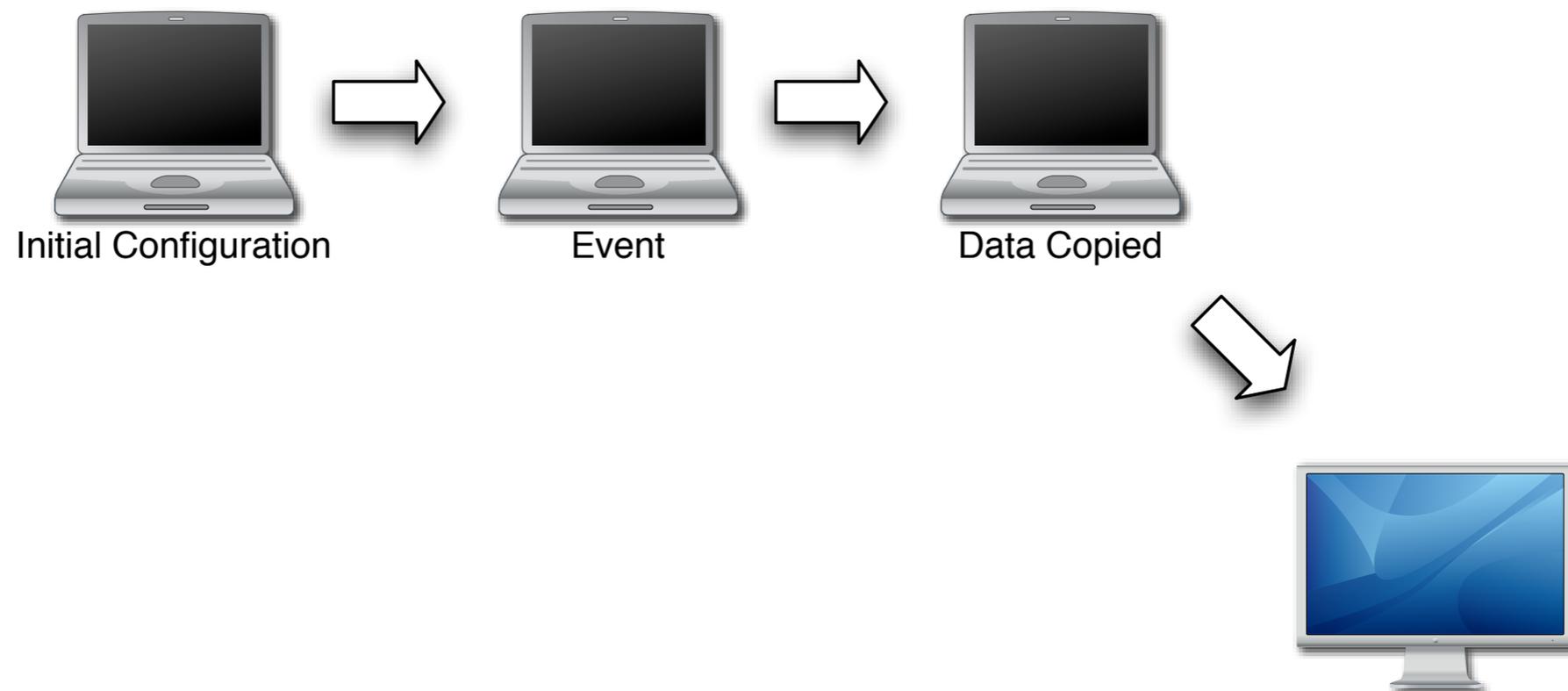
Alternative explanations:

- The file was listed 57 minutes later.
- The file was modified on a different day
- The computer's clock was changed before the file was modified and/or listed.
- The whole example was faked.

When we look at a computer system, we build a *hypothesis* about the computer's past.

The hypothesis makes assumptions about:

- The hardware under investigation.
- The software under investigation.
- The flow of time.
- The movement of the evidence
- The system being used to investigate the data



Usually the assumptions are accurate.
Sometimes they are not.



Other assumptions:

- Event didn't fake the initial configuration.
Attacker creates a new vulnerability to hide one actually used.
- All programs used by attacker were copied.
Program might be hidden in the graphics co-processor.
- Analysis system is faithful and accurate.
Attacker's tools might be invisible due to a bug in the forensic tool.

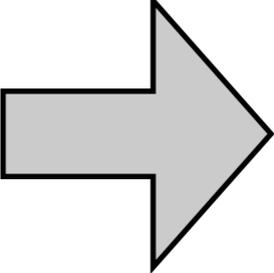


See: *A Hypothesis-Based Approach to Digital Forensic Investigations*, Brian D. Carrier, PhD. Thesis, Purdue University, 2006

Digital Forensics has both limitations and advantages compared to traditional forensics.

In the digital domain, a “1” can be changed into a “0” without leaving a trace.

Digital Forensics has both limitations and advantages compared to traditional forensics.

Pencil writing
on paper + Eraser  Erased pencil
writing

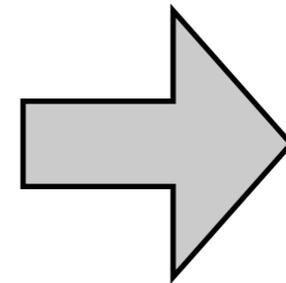
In the digital domain, a “1” can be changed into a “0” without leaving a trace.

Digital Forensics has both limitations and advantages compared to traditional forensics.

Pencil writing
on paper

+

Eraser

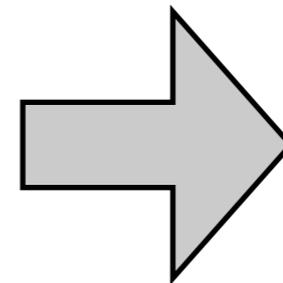


Erased pencil
writing

Word document
on USB drive

+

Drive
Eraser



Blank USB
drive

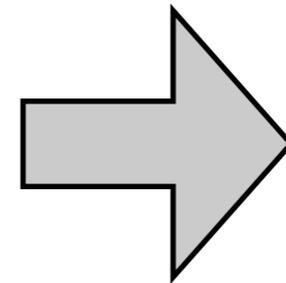
In the digital domain, a “1” can be changed into a “0” without leaving a trace.

Digital Forensics has both limitations and advantages compared to traditional forensics.

Pencil writing
on paper

+

Eraser

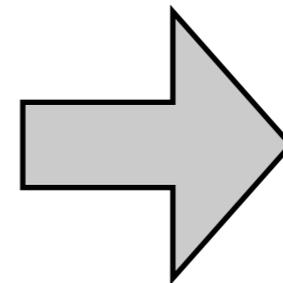


Erased pencil
writing

Word document
on USB drive

+

Drive
Eraser



Blank USB
drive

Digital Forensics has both limitations and advantages compared to traditional forensics.

Pencil writing on paper + Eraser → Erased pencil writing

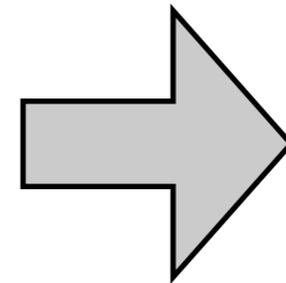
Word document on USB drive + Drive Eraser → Blank USB drive

Digital Forensics has both limitations and advantages compared to traditional forensics.

Pencil writing
on paper

+

Eraser

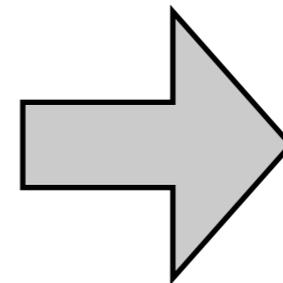


Erased pencil
writing

Word document
on USB drive

+

Drive
Eraser



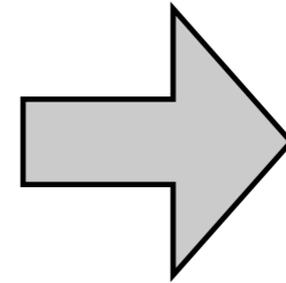
Blank USB
drive

Digital Forensics has both limitations and advantages compared to traditional forensics.

Pencil writing
on paper

+

Eraser

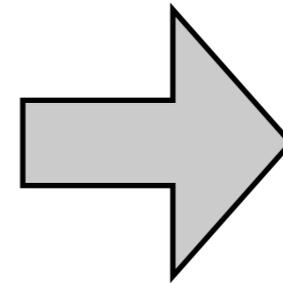


Erased pencil
writing

Word document
on USB drive

+

Drive
Eraser



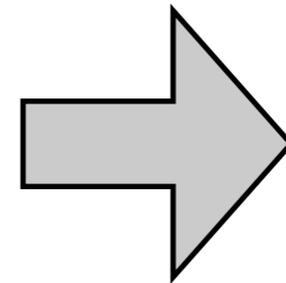
Blank USB
drive

Digital Forensics has both limitations and advantages compared to traditional forensics.

Pencil writing
on paper

+

Eraser

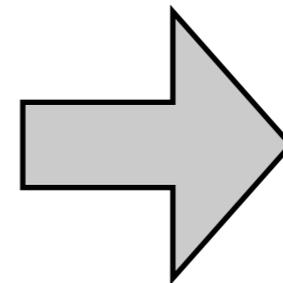


Erased pencil
writing

Word document
on USB drive

+

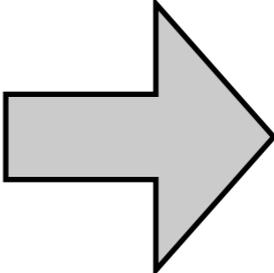
Drive
Eraser



Blank USB
drive

In the digital domain,
it can be very hard to find all the copies and traces of a piece of information.

Digital Forensics has both limitations and advantages compared to traditional forensics.

Word document
on USB drive + Drive
Eraser  Blank USB
drive

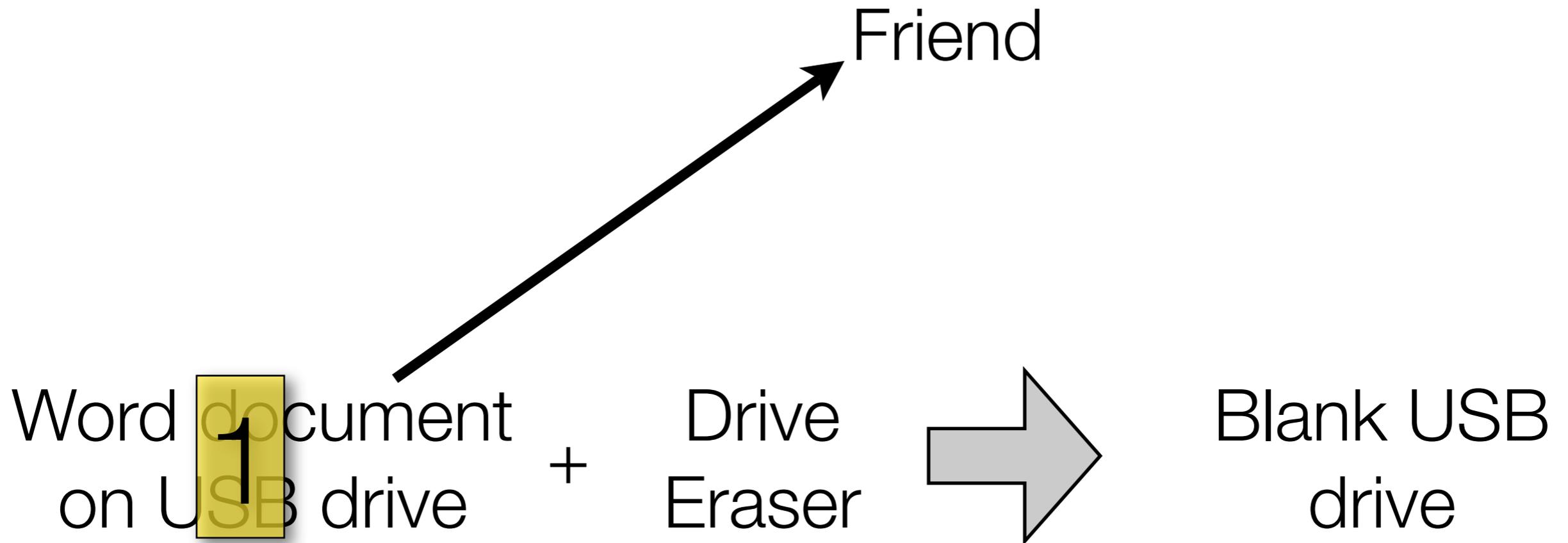
In the digital domain,
it can be very hard to find all the copies and traces of a piece of information.

Digital Forensics has both limitations and advantages compared to traditional forensics.



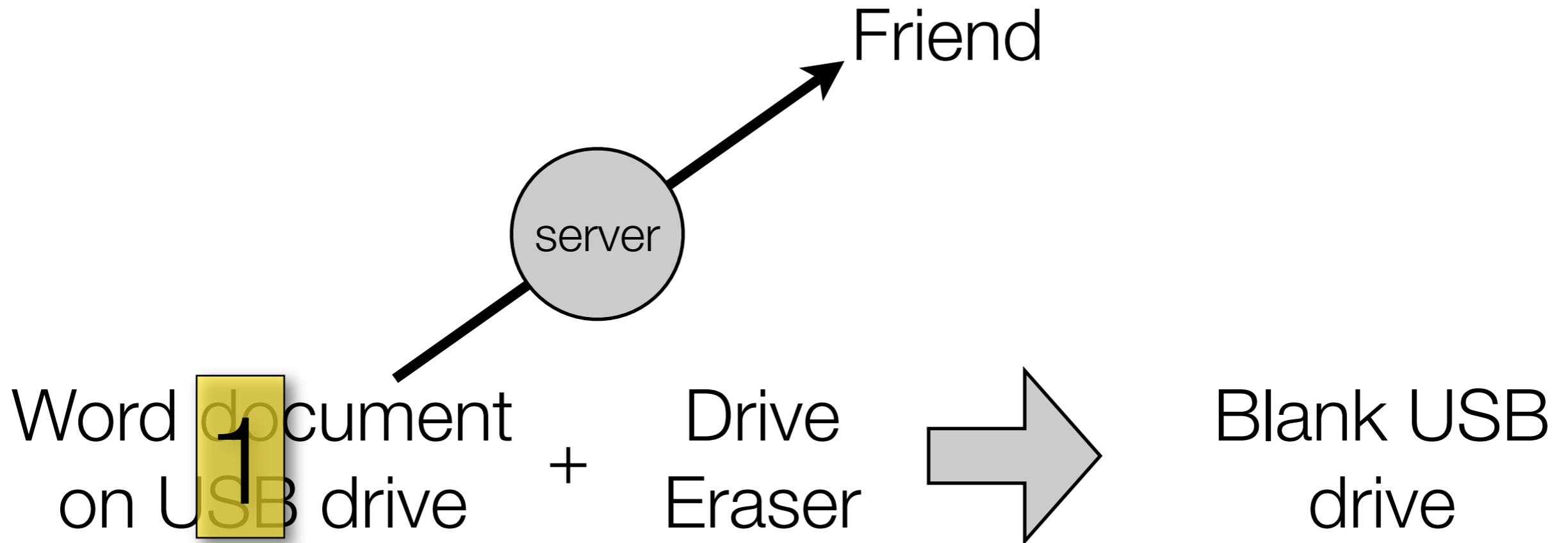
In the digital domain,
it can be very hard to find all the copies and traces of a piece of information.

Digital Forensics has both limitations and advantages compared to traditional forensics.



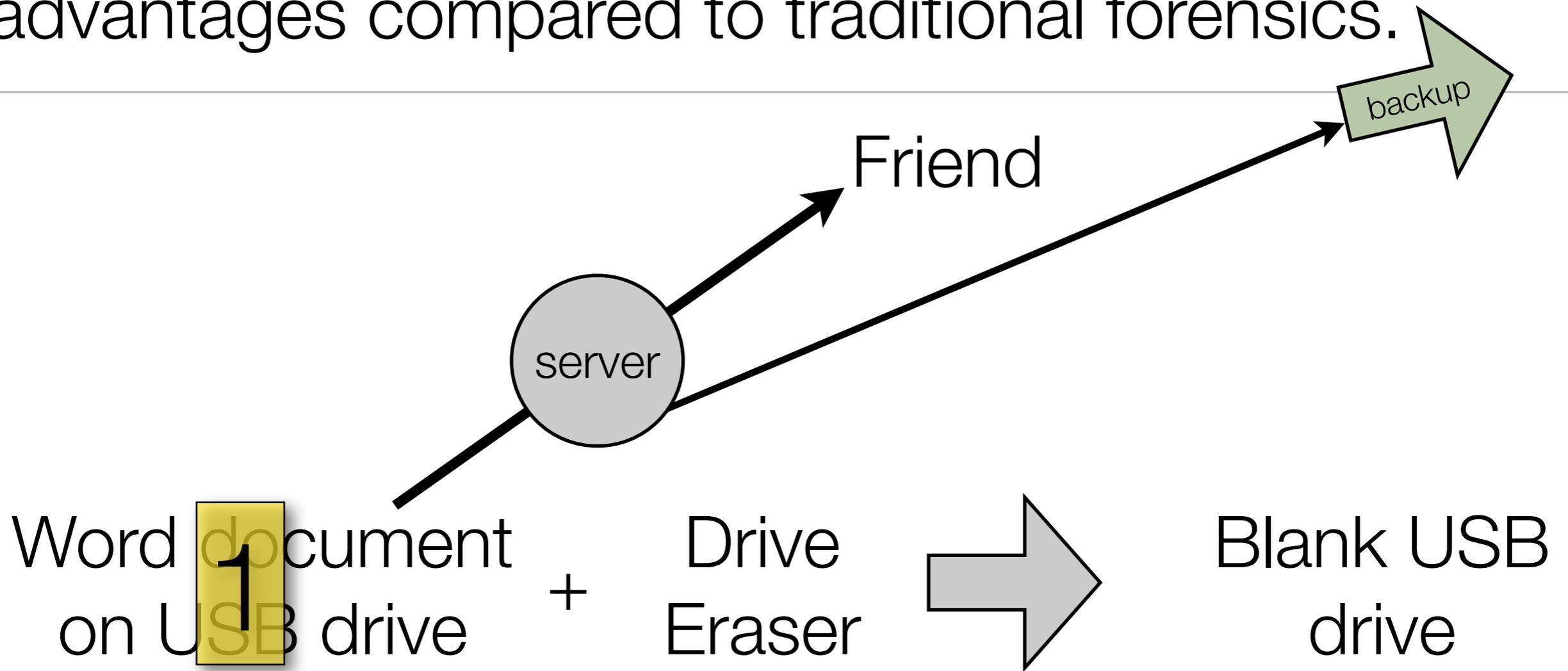
In the digital domain,
it can be very hard to find all the copies and traces of a piece of information.

Digital Forensics has both limitations and advantages compared to traditional forensics.



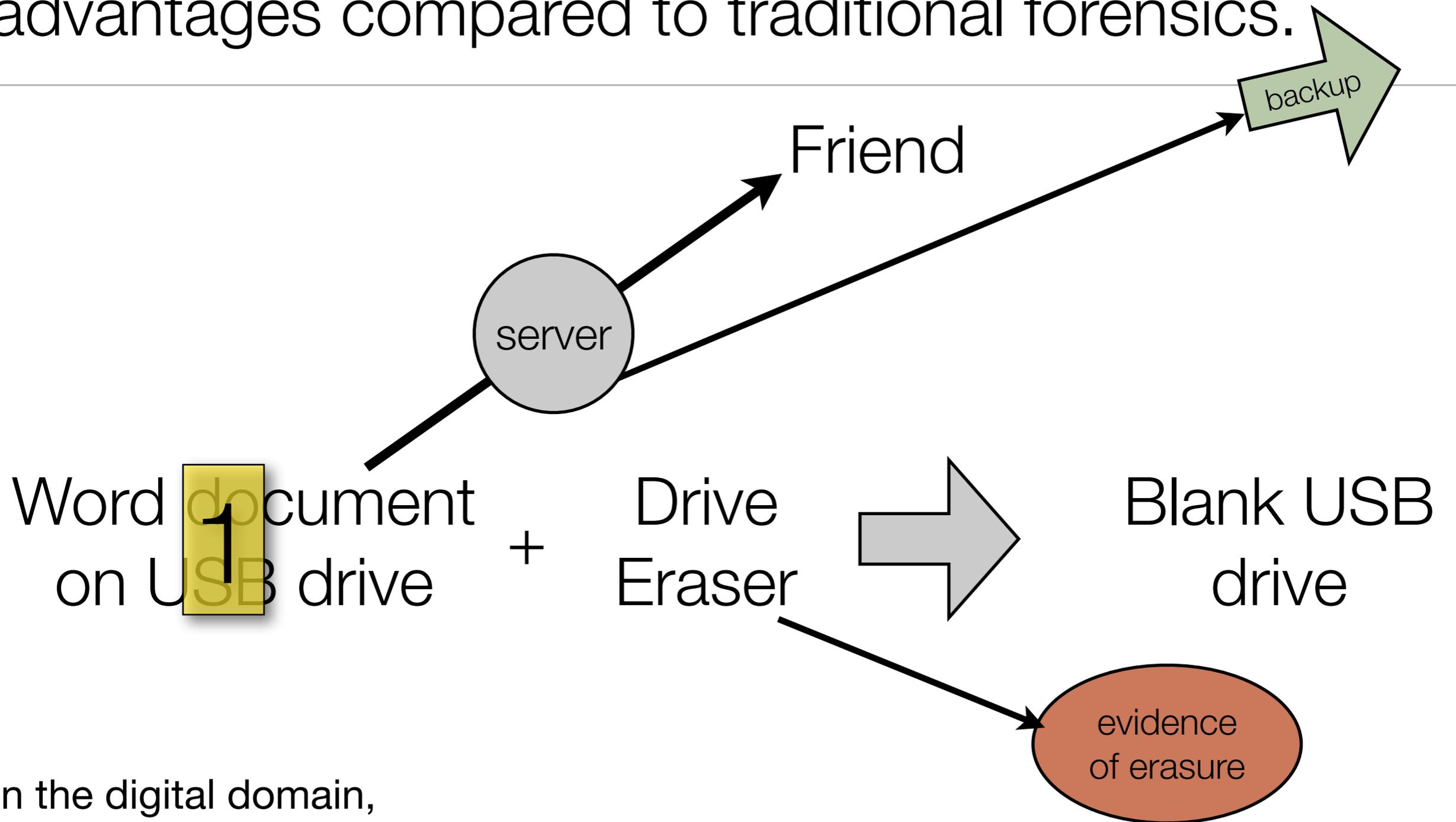
In the digital domain,
it can be very hard to find all the copies and traces of a piece of information.

Digital Forensics has both limitations and advantages compared to traditional forensics.



In the digital domain,
it can be very hard to find all the copies and traces of a piece of information.

Digital Forensics has both limitations and advantages compared to traditional forensics.



In the digital domain, it can be very hard to find all the copies and traces of a piece of information.

Forensics has many uses beyond the courtroom

Data Recovery

Testing and Evaluating:

- System Performance
- Privacy Properties & Tools
- Security Policies

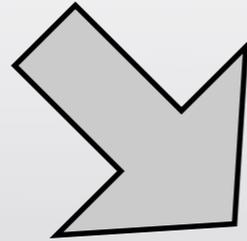
Spot-check regulatory compliance:

- Internal information flows
- Data flow across network boundaries
- Disposal policies

Performance Evaluation

Information Exploitation





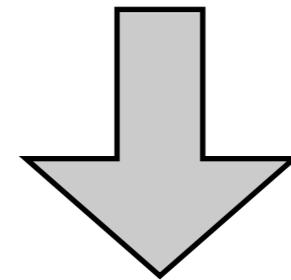
The Forensic Process

From computer to courtroom.
The Investigation.
The “Hacker Defense.”

Computer Forensics turns computer systems into courtroom testimony.

Five basic steps:

- 1.Preparation
- 2.Collection
- 3.Examination
- 4.Analysis
- 5.Reporting



Source:

Electronic Crime Scene Investigation Guide,
National Institute of Justice

Step 1: Preparation

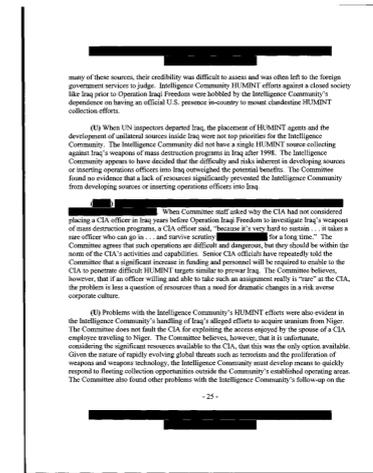
Identify potential sources of evidence

Computer system components:

- Hard drives
- Memory / flash / configuration
- Physical configuration

Other data sources:

- Web Pages
- Files
- Communication networks



Each source may need its own personnel, tools, training & procedures.
One of the most difficult tasks is determining what to include & exclude.

Step 2: Collect and Preserve the evidence

If the activity is ongoing, your choices include:

- Passive Monitoring
- Experimental Probing

If the activity is over, choices include:

- Make a copy
- Seizure

Issues to consider:

- What tools are used? Are they validated?
- Is the copy accurate? Is it complete?
- How can you prove that the copy wasn't modified at a later time?



Tools must be validated so their results can be trusted.

Validation is a series of tests to prove the tool produces **consistent** and **accurate** results.

Validation can discover errors in tools or procedures.

NIST's Information Technology Laboratory
Computer Forensics Tool Testing Program
has validated *some* tools.



<http://www.cftt.nist.gov/>

Step 3: Examination.

Make evidence “visible” and eliminate excess.

Disk Analysis:

- Examine partitions and file systems
- Resident & delete files
- “Slack space” at end of files
- Unallocated space between files

File based evidence:

- Document text
- Deleted text
- Metadata (creation date; author fields; etc.)

Network Evidence:

- Device configuration
- Categorize packets; discard what isn't needed

Step 4: Analyze to determine “significance and probative value”

Build a hypothesis about what happened.

Look for evidence to prove or disprove hypothesis.

Examples:

- Hypothesis: Suspect broke into a telephone company computer and stole confidential documents.
- Evidence: Hacker tools; confidential information from telco.

- Hypothesis: Suspect is arrested on suspicion of child pornography
- Evidence: Known child pornography on suspect’s hard drive

BUT:

Investigators rarely look for counter-evidence.

Build a hypothesis about what happened.

Look for evidence to prove or disprove hypothesis.

Examples:

- Hypothesis: Suspect broke into a telephone company computer and stole confidential documents.
- Evidence: Hacker tools; confidential information from telco.
- **Counter Evidence: Documents publicly available**

- Hypothesis: Suspect is arrested on suspicion of child pornography
- Evidence: Known child pornography on suspect's hard drive
- **Counter Evidence: Hacker software allowing remote access**

Counter Evidence:
Trojan allowed remote access

Counter Evidence: Trojan allowed remote access

Aaron Caffrey, 19, charged with crashing systems at the port of Houston, TX.

- Caffrey claimed that hackers had broken into his computer and used it as a launch pad.
- Jury acquits, October 2003.

Counter Evidence:

Trojan allowed remote access

Aaron Caffrey, 19, charged with crashing systems at the port of Houston, TX.

- Caffrey claimed that hackers had broken into his computer and used it as a launch pad.
- Jury acquits, October 2003.

United States v. Michael McCourt,
US Court of Appeals Case 061018P 11/24/06

- Defendant claimed hacker put hundreds of child pornography videos and stills on his computer.
- Appellate court ruled that defendant knew files were there, no matter how they got there.
- Hacker defense failed.
- <http://www.ca8.uscourts.gov/opndir/06/11/061018P.pdf>

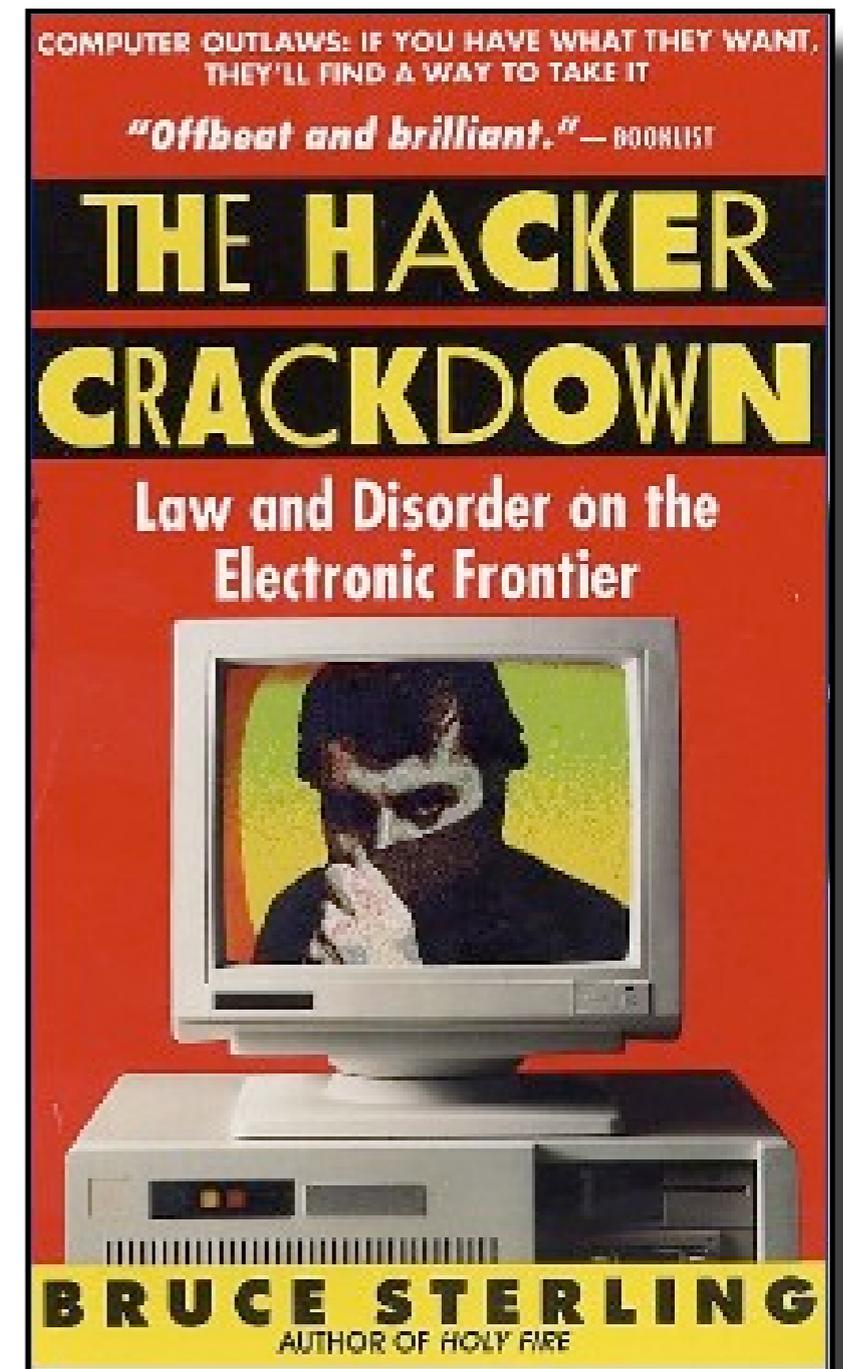
The Hacker Defense: Indications & Contradictions

Try the hacker defense when:

- The system has a Trojan on it.
- The suspect has an alibi (e.g., lunch with a friend at a restaurant.)

Avoid the hacker defense when:

- The child porn was copied to CDRs and stored under the suspect's bed.
- The suspect is a hacker or sysadmin (already has hacker tools.)



Step 5: Reporting and Testimony

Many kinds of testimony:

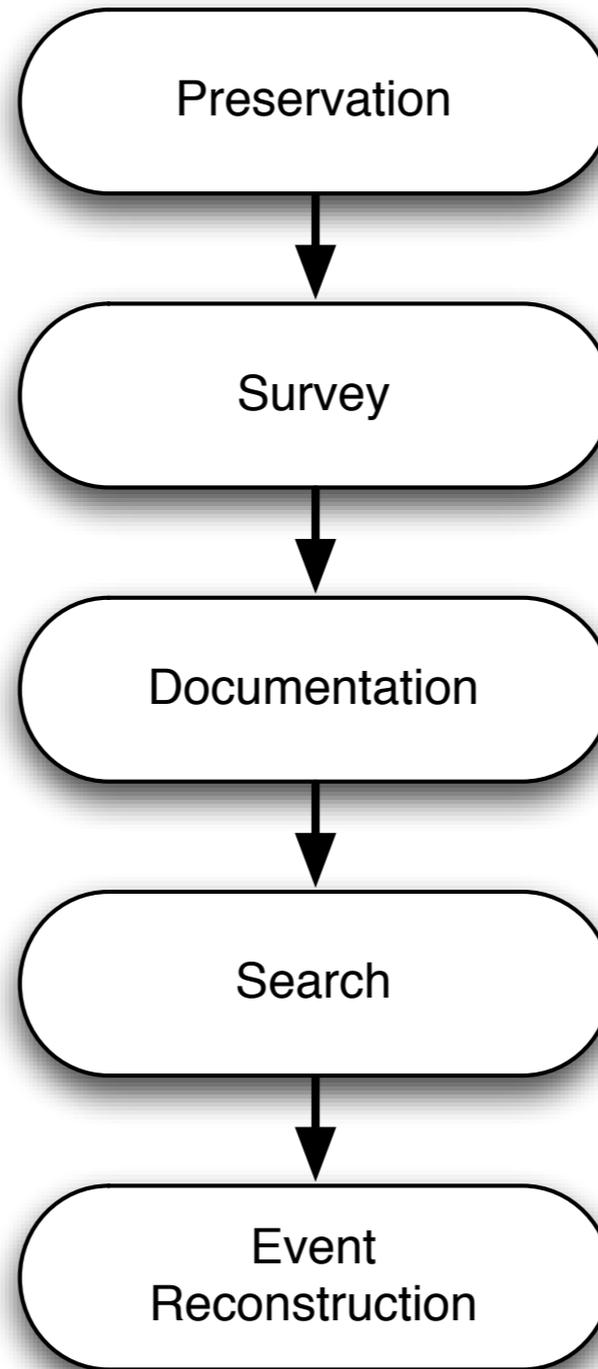
- Written reports
- Depositions
- Courtroom testimony



Testimony needs to include several key points:

- The tools used and procedures that were followed
- What was found
- Examiner's interpretation of what it means

Carrier & Spafford's Digital Crime Scene Investigation model has five similar steps:



This isn't really what happens in reality.
Instead, investigations are guided by "hypotheses."

Goal of most investigations is to explain evidence that is observed.

- Investigations asked to answer questions about previous states or events.
- Investigator encounters the machine.
- Investigator uses tools to extract and preserve information from machine

"Because the observation of the data is indirect, a hypothesis must be formed that the actual data is equal to the observed data"

"Hypotheses also need to be formulated about the data abstractions that exist and the previous states and events that occurred."

- The investigator searches for data that supports or refutes the hypotheses.
- Information may be used for confirming/eliminating a hypotheses even if the information itself is inadmissible in court.

A Hypothesis-Based Approach to Digital Forensic Investigations,
Brian D. Carrier, PhD Thesis, June 2006



Legal Standards

US Federal Rules of Evidence
Daubert
Access & Search Warrants

US Federal Rules of Evidence

Article VIII regulates the testimony of “experts”

Rule 702. Testimony by Experts

Rule 703. Bases of Opinion Testimony by Experts

Rule 704. Opinion on Ultimate Issue

Rule 705. Disclosure of Facts or Data Underlying Expert Opinion

Rule 706. Court Appointed Experts

These rules apply in the Federal Court; many states follow the rules as well

- <http://www.law.cornell.edu/rules/fre/>

Rule 702. Testimony by Experts

“If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if

- (1) the testimony is based upon sufficient facts or data,
- (2) the testimony is the product of reliable principles and methods, and
- (3) the witness has applied the principles and methods reliably to the facts of the case.”

Rule 703. Bases of Opinion Testimony by Experts

“The facts or data in the particular case upon which an expert bases an opinion or inference may be those perceived by or made known to the expert at or before the hearing.

If of a type reasonably relied upon by experts in the particular field in forming opinions or inferences upon the subject, the facts or data need not be admissible in evidence in order for the opinion or inference to be admitted.

Facts or data that are otherwise inadmissible shall not be disclosed to the jury by the proponent of the opinion or inference unless the court determines that their probative value in assisting the jury to evaluate the expert's opinion substantially outweighs their prejudicial effect.”

Rule 704. Opinion on Ultimate Issue

(a) Except as provided in subdivision (b), testimony in the form of an opinion or inference otherwise admissible is not objectionable because it embraces an ultimate issue to be decided by the trier of fact.

(b) No expert witness testifying with respect to the mental state or condition of a defendant in a criminal case may state an opinion or inference as to whether the defendant did or did not have the mental state or condition constituting an element of the crime charged or of a defense thereto. Such ultimate issues are matters for the trier of fact alone.

The “Daubert Standard” is designed to keep “junk science” out of the courts.

Daubert turns federal judges “gatekeepers.”

Daubert v. Merrell Dow Pharmaceuticals, 509 US 579 (1993)

Evidence must be “relevant”

(so as not to waste the court’s time or confuse matters)

Evidence must be “reliable” (ie, scientific)

- Subject to peer review (has been published)
- Generally accepted by the relevant professional community
- Standards for the technique’s operation
- Known error rate

Surprisingly, digital evidence may not meet this standard.

[Carrier 2006, pp. 1-4]

Investigators need access to the digital evidence.

“Consent Searches” — The owner gives consent.

- No warrant or probable cause required; officers not required to warn people of their right to withhold consent (Schneckloth v. Bustamonte).
- Employers can give consent for an employee.
- Spouse may give consent to marital property.
- Parents can give consent for children under 18, and sometimes over 18.
- System Administrators can give consent, but are regulated under the Electronic Communications Privacy Act.

Warrant Searches

- Police swears an oath that proves probable cause or hearsay information.
- Warrant defines the terms of what may be searched and seized.

Warrantless Searches

- Everything else.

US Law allows searching evidence in “plain view” without a warrant.

According to *Searching and Seizing Computers* (US DoJ 2002):

- Agent must be in lawful position to observe and access the evidence
- Incriminating character must be immediately apparent.
- Plain view cannot justify violation of a person’s “reasonable expectation of privacy.”
- Government cannot “justify opening a closed computer file it is not otherwise authorized to view”

Be careful with “plain view.”

Be careful with “plain view.”

US v. Carey, 172 F.3d 1268 (10th Cir. 1999)

- Investigator executing warrant on narcotics case finds two computers.
- Investigators seize computers looking for narcotics information. Obtain warrant to search for drug information.
- Investigators discover “JPG” files with child pornography;
- Focuses on child porn.
- Court throws out conviction; search beyond original consent and warrant.

Be careful with “plain view.”

US v. Carey, 172 F.3d 1268 (10th Cir. 1999)

- Investigator executing warrant on narcotics case finds two computers.
- Investigators seize computers looking for narcotics information. Obtain warrant to search for drug information.
- Investigators discover “JPG” files with child pornography;
- Focuses on child porn.
- Court throws out conviction; search beyond original consent and warrant.

US v. Gray, 78 F.Supp. 2d 524 (E.D. Virginia, 1999)

- FBI examining a computer system for evidence of “hacking” file child pornography in a subdirectory.
- Discovery was “inadvertent;” investigation continued original search
- Files may be mislabeled; investigators may view every file on computer

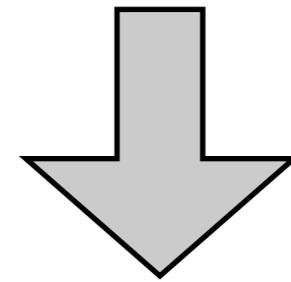
Summary: The Forensic Process

Purpose of Computer Forensics is to get evidence from the computer to the court room.



Training, Preparation & Process

Federal Rules of Evidence governs use of technology & testimony

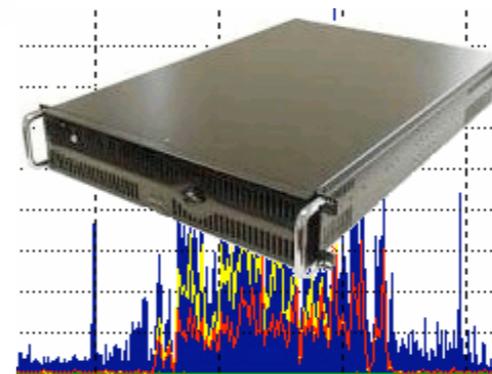


Tutorial Roadmap...

- ✓ Introduction
- ✓ The Forensic Process
- ✓ Legal Standards
- 3. Specific Forensic Techniques

- Disk Forensics
- Network Forensics
- Document Forensics
- Memory Forensics
- Cell Phone Forensics
- Software Forensics

4. Anti-Forensics



```
printf("%d, %f", i, f);  
    i++; f+=3.0;  
    g = fmod(f,i);
```

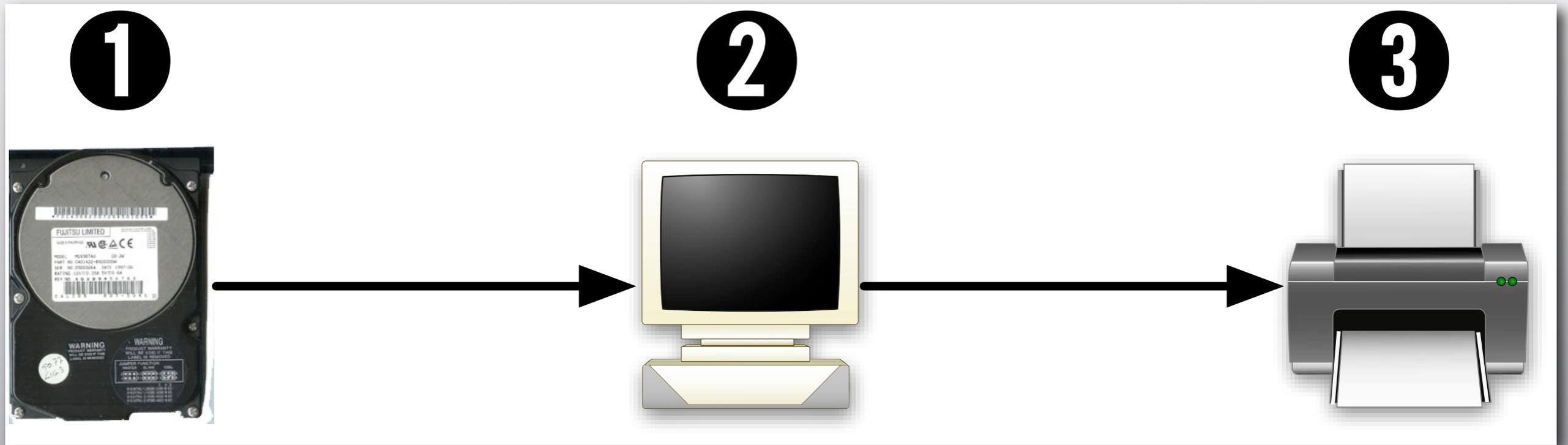
many of these sources, their credibility was difficult to assess and was often left to the foreign government services to judge. Intelligence Community HUMINT efforts against a blood society like Iraq prior to Operation Iraqi Freedom were hampered by the Intelligence Community's dependence on having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

(b) When UN inspectors departed Iraq, the placement of HUMINT agents and the development of unaffiliated 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 risk 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.

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 was hard to maintain... it takes a rare officer who can go in... and survive scrutiny... for a long time." The Committee agrees that such operations are difficult and dangerous, but they should be within the scope of the CIA's activities and capabilities. Some CIA officials have repeatedly told the Committee that a significant increase in funding and personnel will be required to enable the CIA to possess sufficient HUMINT assets similar to those of the Intelligence Community, 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.

(c) 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 -



Disk Forensics

Tools
Residual Data
Remnant Data

Disk forensics: Typical tasks

Recover:

- Deleted files
- Child pornography

Recreate:

- Timelines - when did the computer do what?
- Flow of information
- Evidence of Inappropriate use

Gather Intelligence:

- Names of associates
- Meeting places

Disk forensics: Tools of the trade

Acquisition Tools:

- Write-Blockers prevent modification
- Network agents allow capture over a network
- Information stored in an “image file” or on a “mirror disk.”

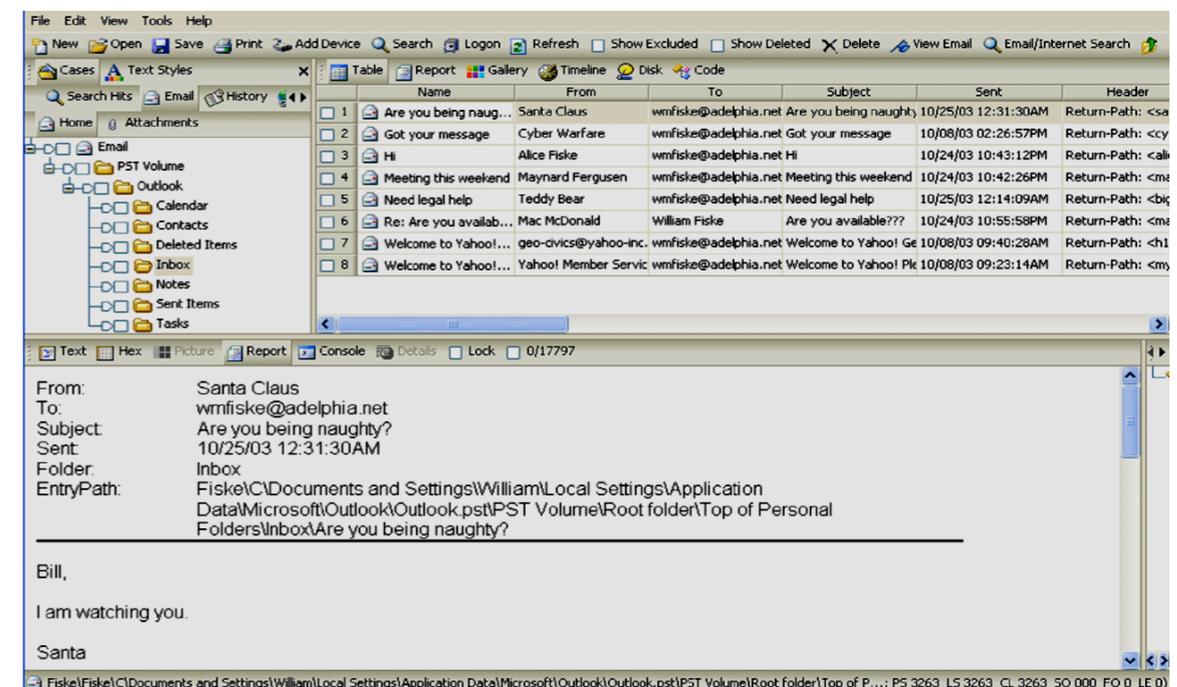


Image File Formats:

- raw, EnCase (E01), AFF, “sgzip”

Analysis Programs:

- The Sleuth Kit (Carrier, Open Source)
- Encase (Guidance Software)
- Forensic Toolkit (Accessdata)



The important thing about disk imaging:

get the data off the suspect's drive, onto your drive.

Imaging options:

- `dd if=/dev/hda of=diskfile.img`
- `aimage /dev/hda diskfile.img`
- LinEn

Most tools will:

- Copy the raw device to a file
- Compute MD5 & SHA1

Some tools will:

- Compress image
- Capture metadata like s/n
- Record investigative notes



You have many options once data is imaged.

Typical “first steps” include:

- Inventory all files (resident & deleted) on disk
- Show files modified during a certain time period
- Eliminate “known goods” (operating system files, etc.)
- Search for “known bads” (hacker tools, child porn)
- Scan for key words, email addresses

Deleted files can be recovered because “delete” doesn’t really delete, it unlinks.

directory

directory

•

• •

Deleted files can be recovered because “delete” doesn’t really delete, it unlinks.



directory

directory

•

• •

```
copy a:file.doc \dir
```

Deleted files can be recovered because “delete” doesn’t really delete, it unlinks.

directory

directory

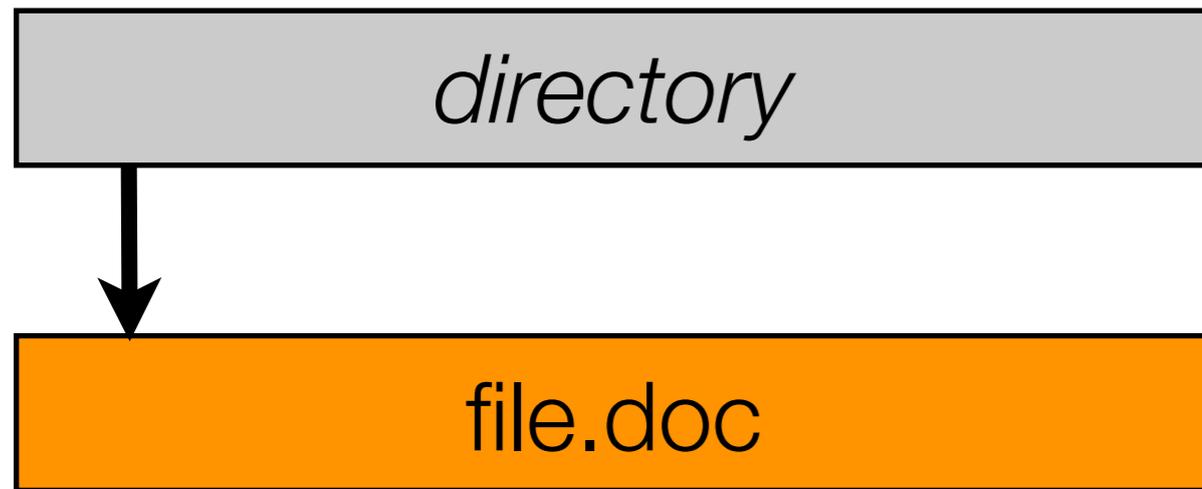
•

• •

file.doc

```
copy a:file.doc \dir
```

Deleted files can be recovered because “delete” doesn’t really delete, it unlinks.



directory

•

• •

`file.doc`

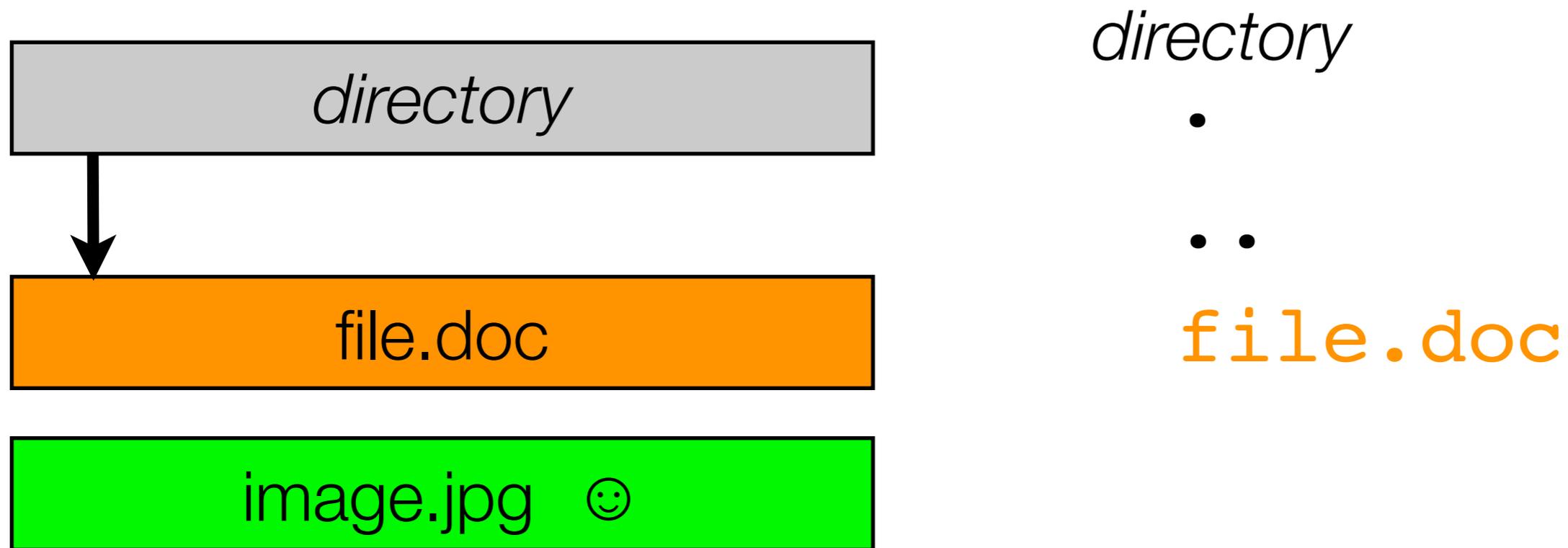
```
copy a:file.doc \dir
```

Deleted files can be recovered because “delete” doesn’t really delete, it unlinks.



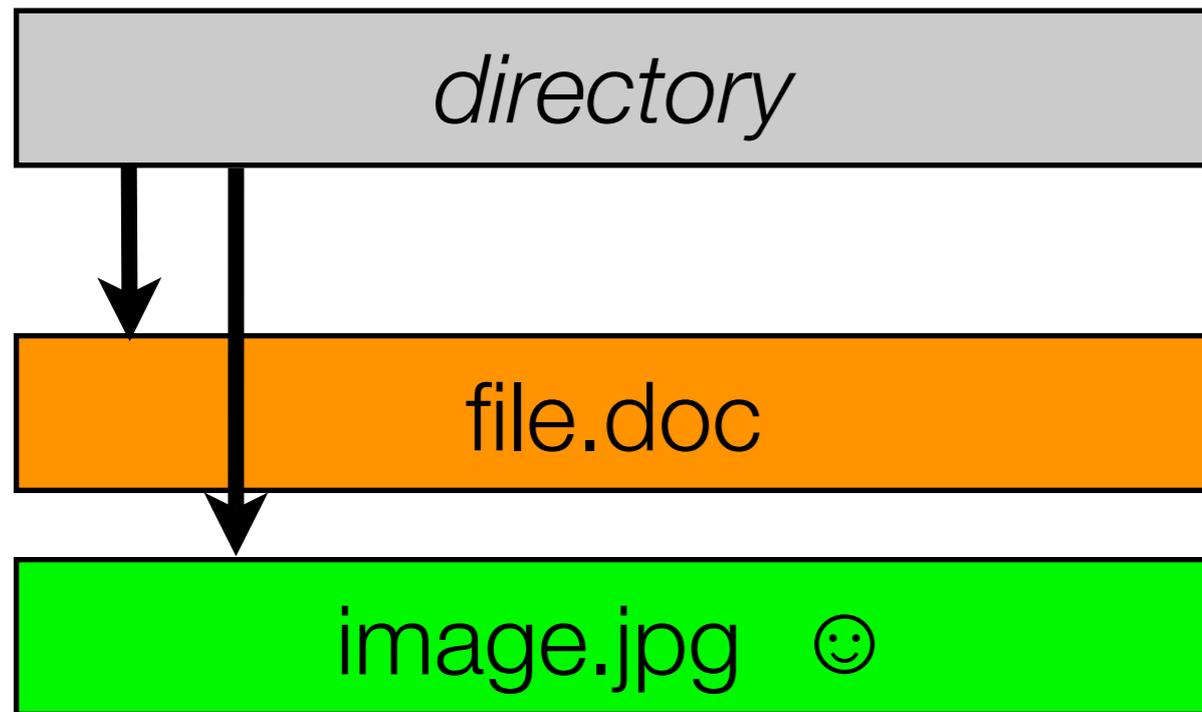
```
copy a:file.doc \dir  
copy a:image.jpg \dir
```

Deleted files can be recovered because “delete” doesn’t really delete, it unlinks.



```
copy a:file.doc \dir
copy a:image.jpg \dir
```

Deleted files can be recovered because “delete” doesn’t really delete, it unlinks.



directory

•

• •

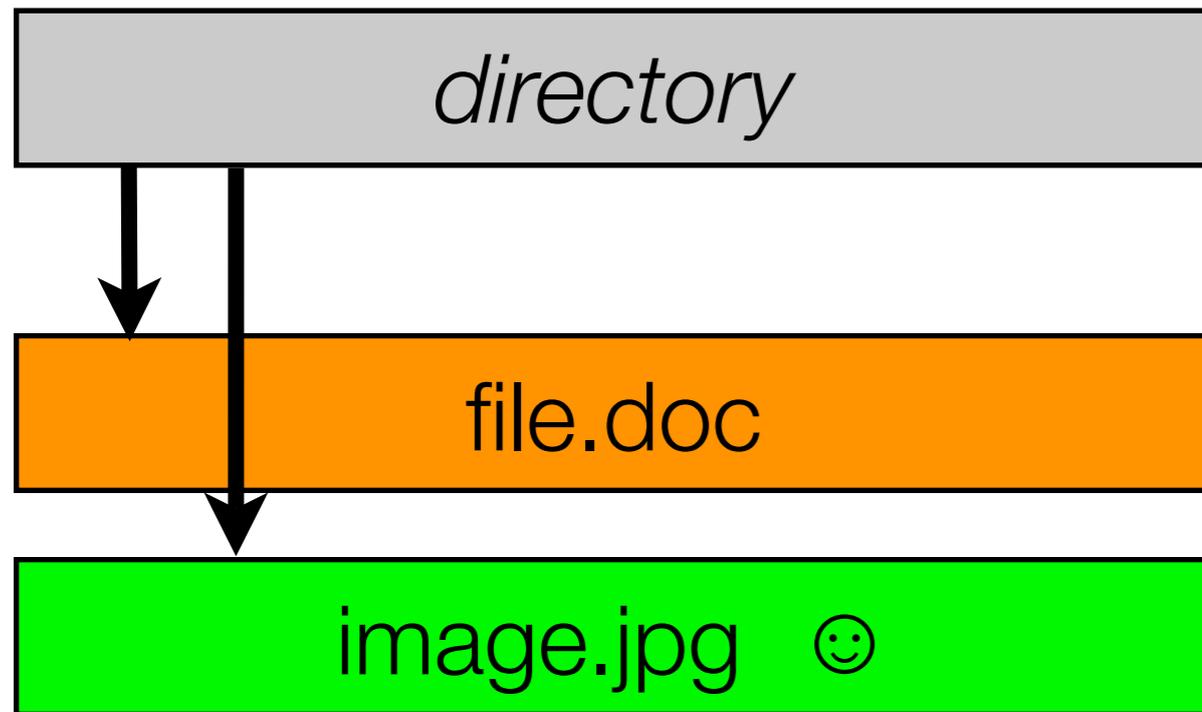
file.doc

image.jpg

```
copy a:file.doc \dir
```

```
copy a:image.jpg \dir
```

Deleted files can be recovered because “delete” doesn’t really delete, it unlinks.



directory

•

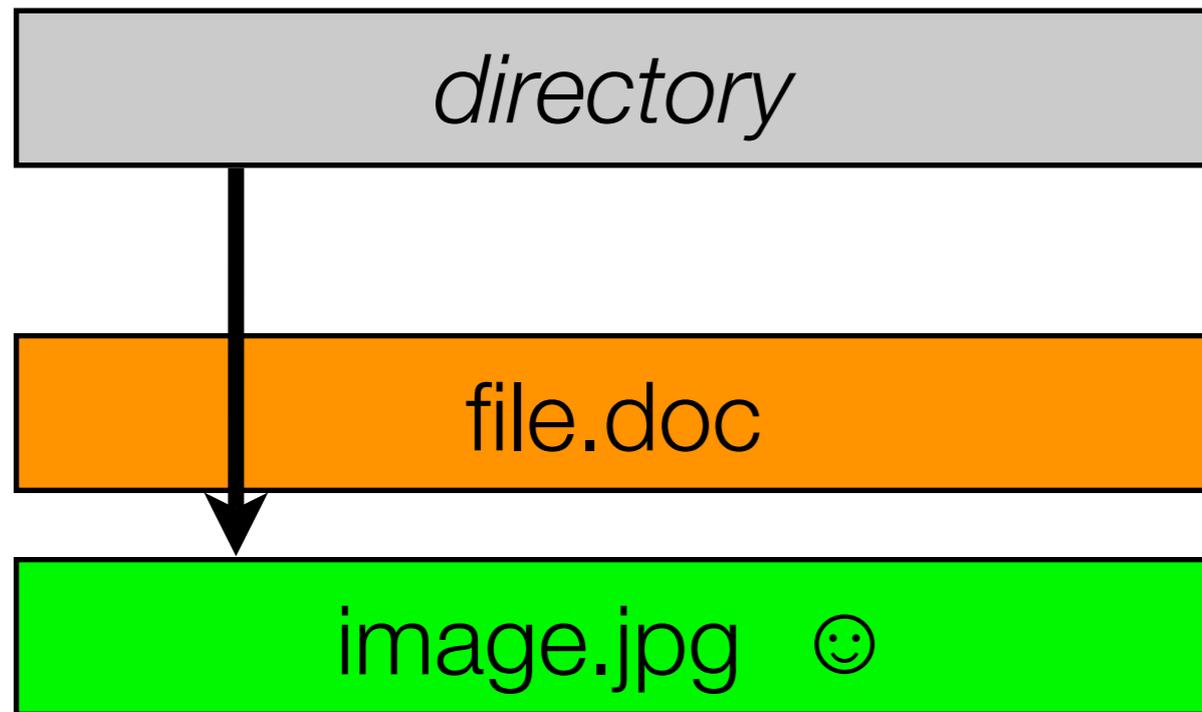
• •

file.doc

image.jpg

```
copy a:file.doc \dir
copy a:image.jpg \dir
del /dir/file.doc
```

Deleted files can be recovered because “delete” doesn’t really delete, it unlinks.



directory

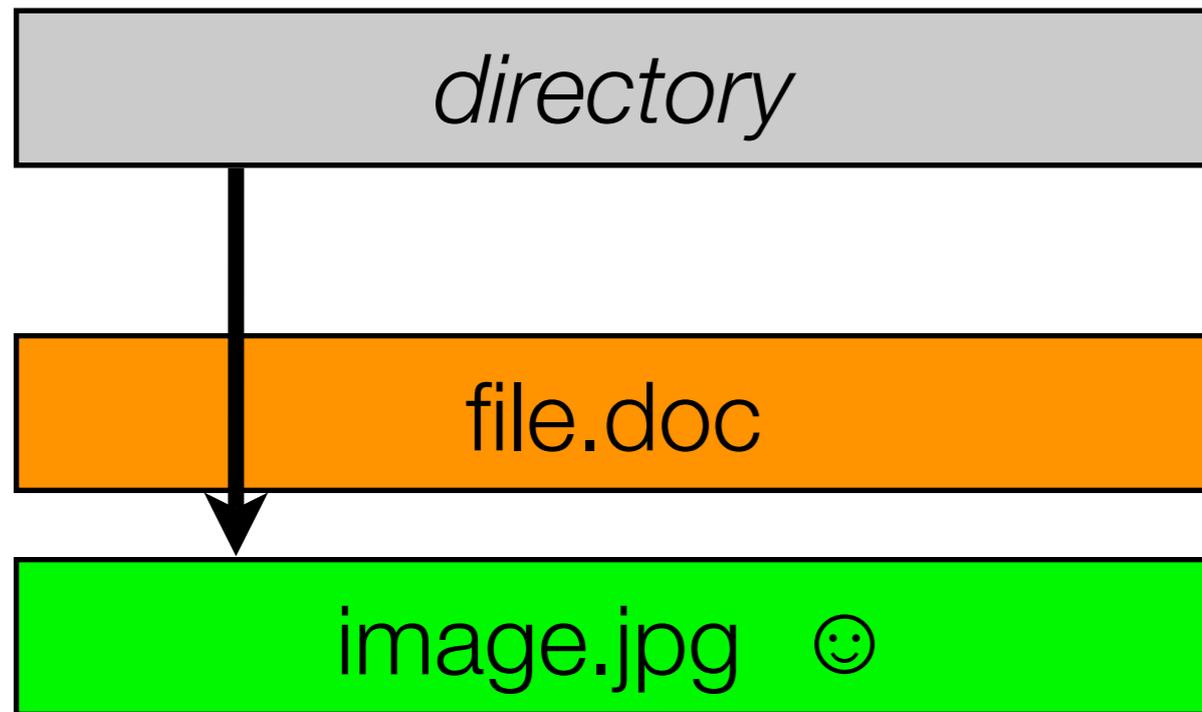
•

• •



```
copy a:file.doc \dir
copy a:image.jpg \dir
del /dir/file.doc
```

Deleted files can be recovered because “delete” doesn’t really delete, it unlinks.



directory

•

• •



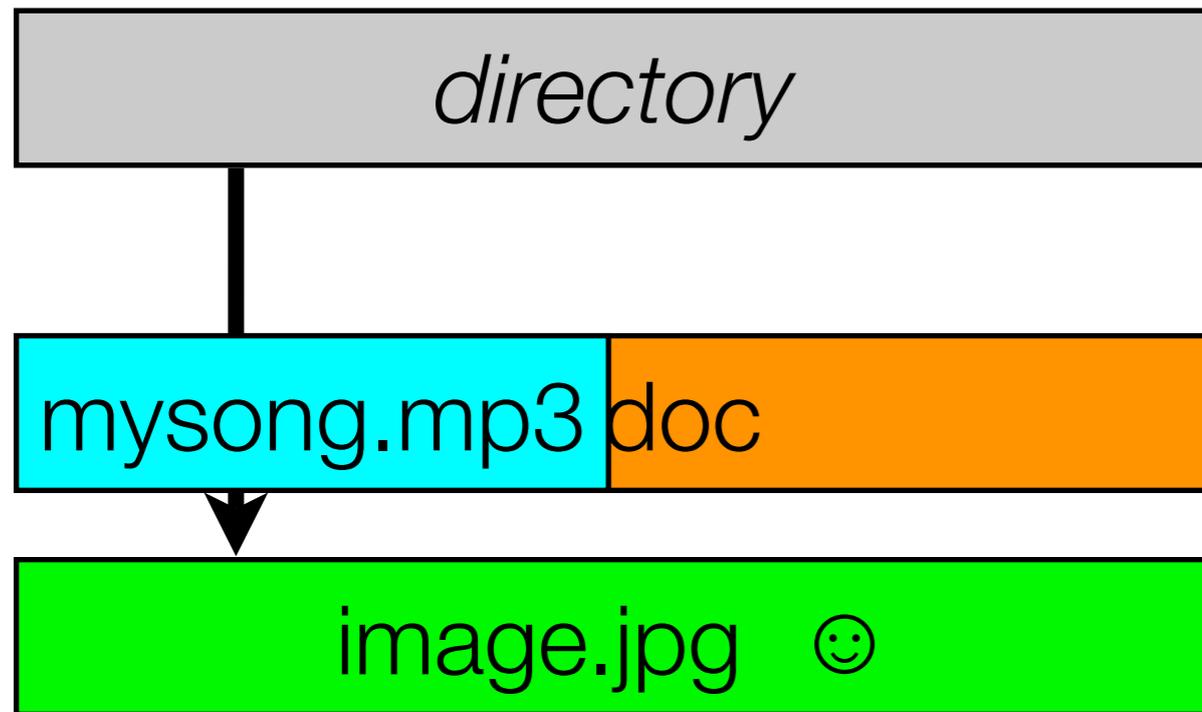
```
copy a:file.doc \dir
```

```
copy a:image.jpg \dir
```

```
del /dir/file.doc
```

```
copy a:mysong.mp3 \dir
```

Deleted files can be recovered because “delete” doesn’t really delete, it unlinks.



directory

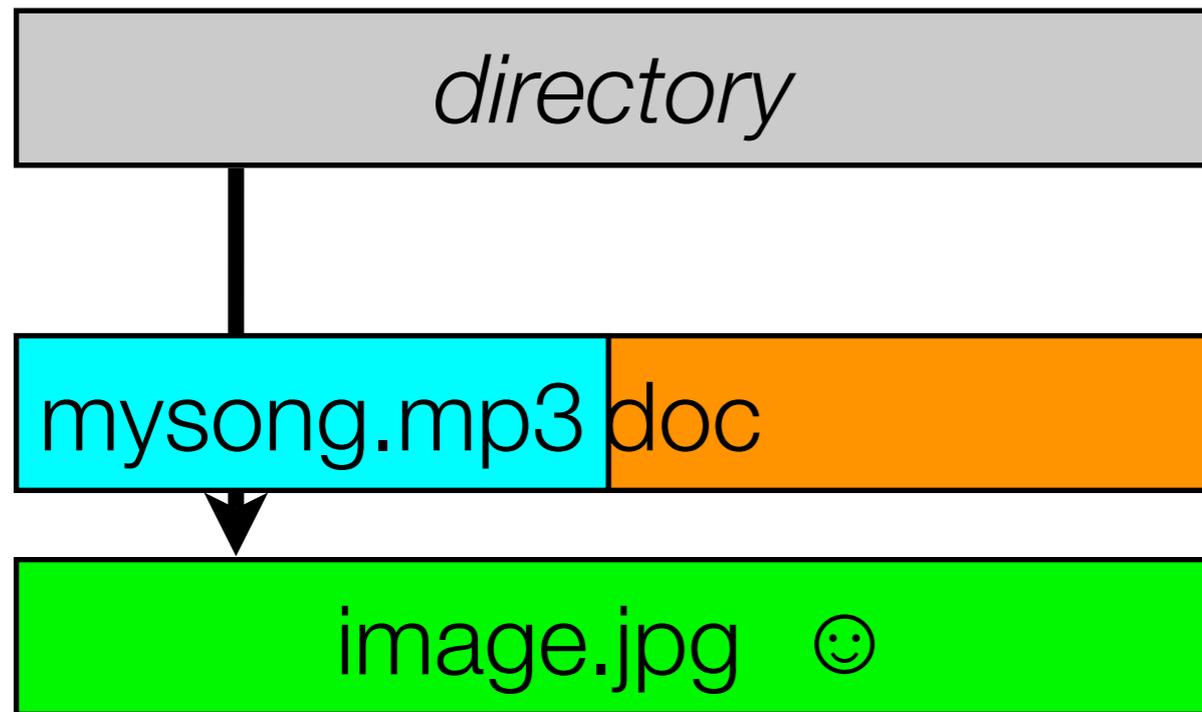
•

• •

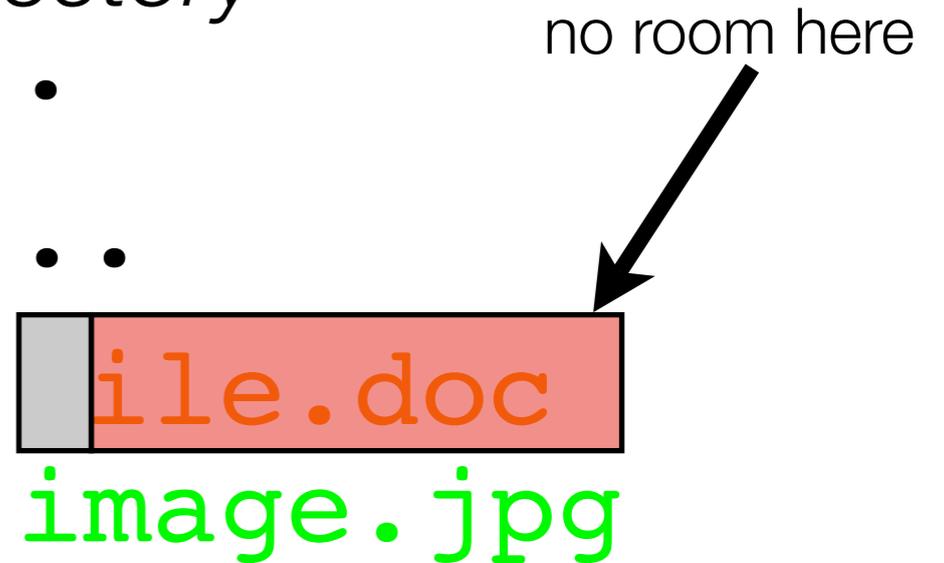


```
copy a:file.doc \dir
copy a:image.jpg \dir
del /dir/file.doc
copy a:mysong.mp3 \dir
```

Deleted files can be recovered because “delete” doesn’t really delete, it unlinks.

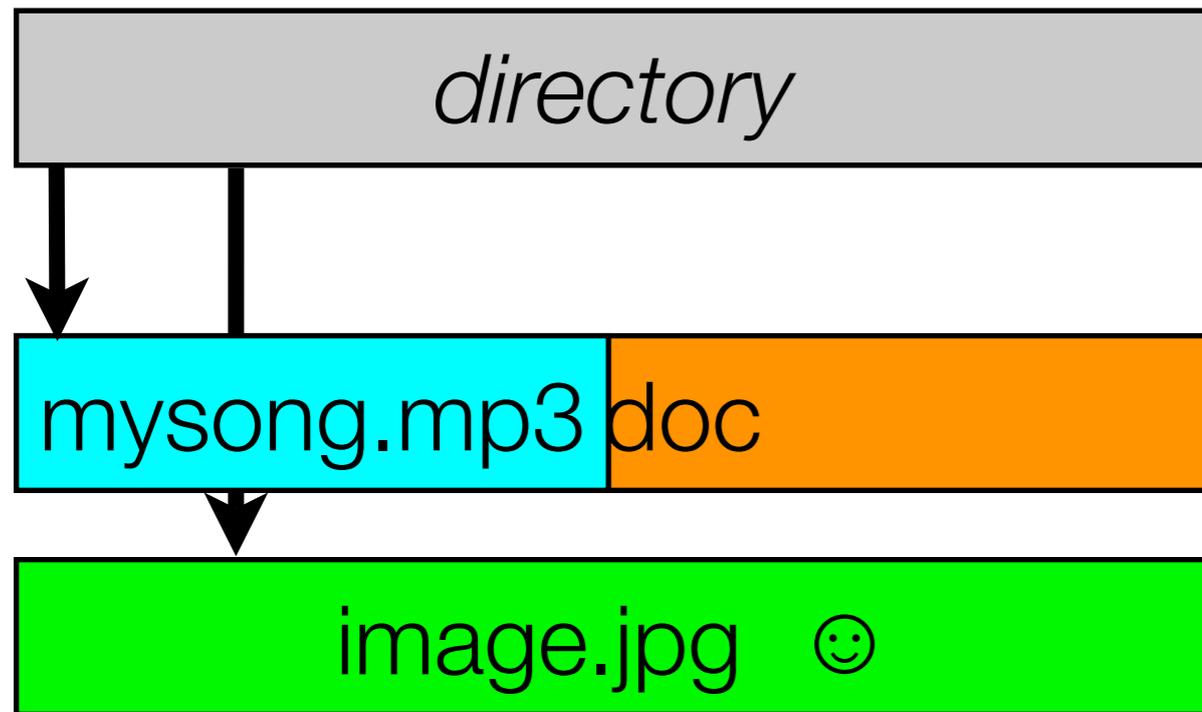


directory

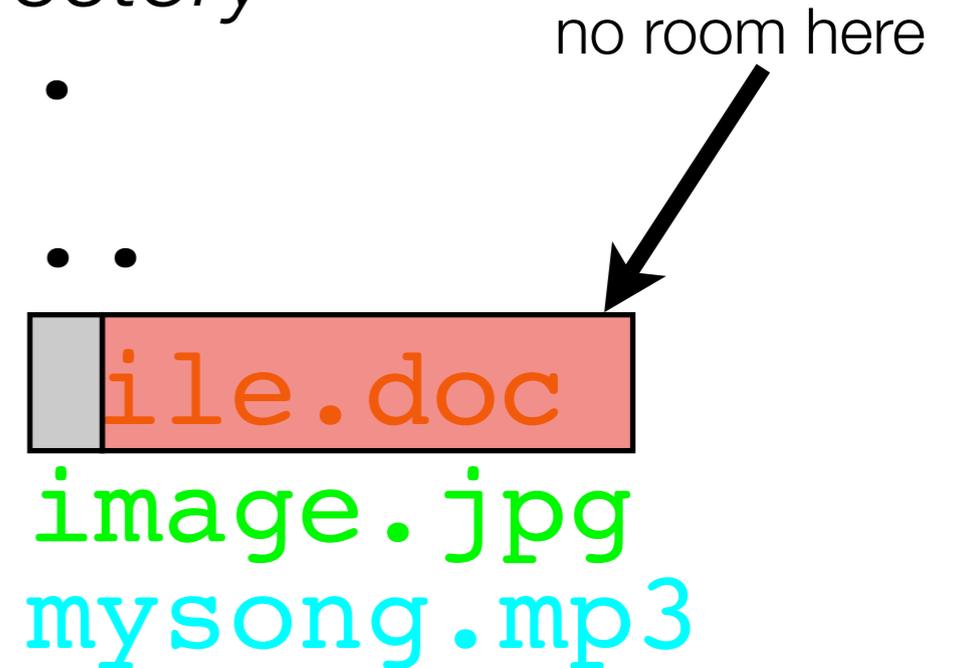


```
copy a:file.doc \dir
copy a:image.jpg \dir
del /dir/file.doc
copy a:mysong.mp3 \dir
```

Deleted files can be recovered because “delete” doesn’t really delete, it unlinks.

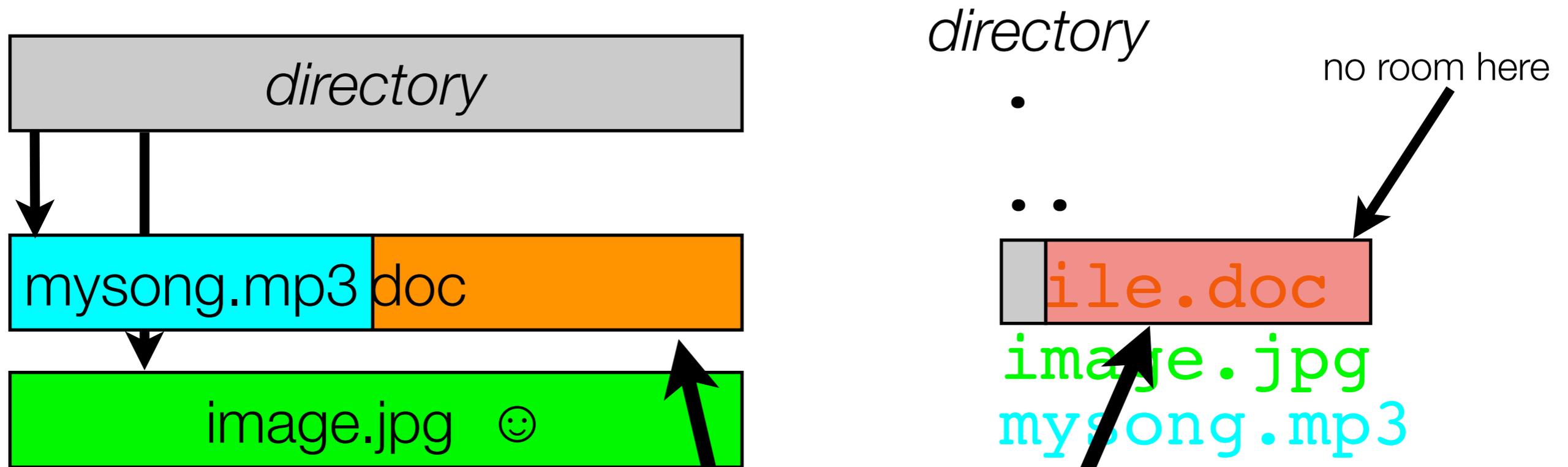


directory



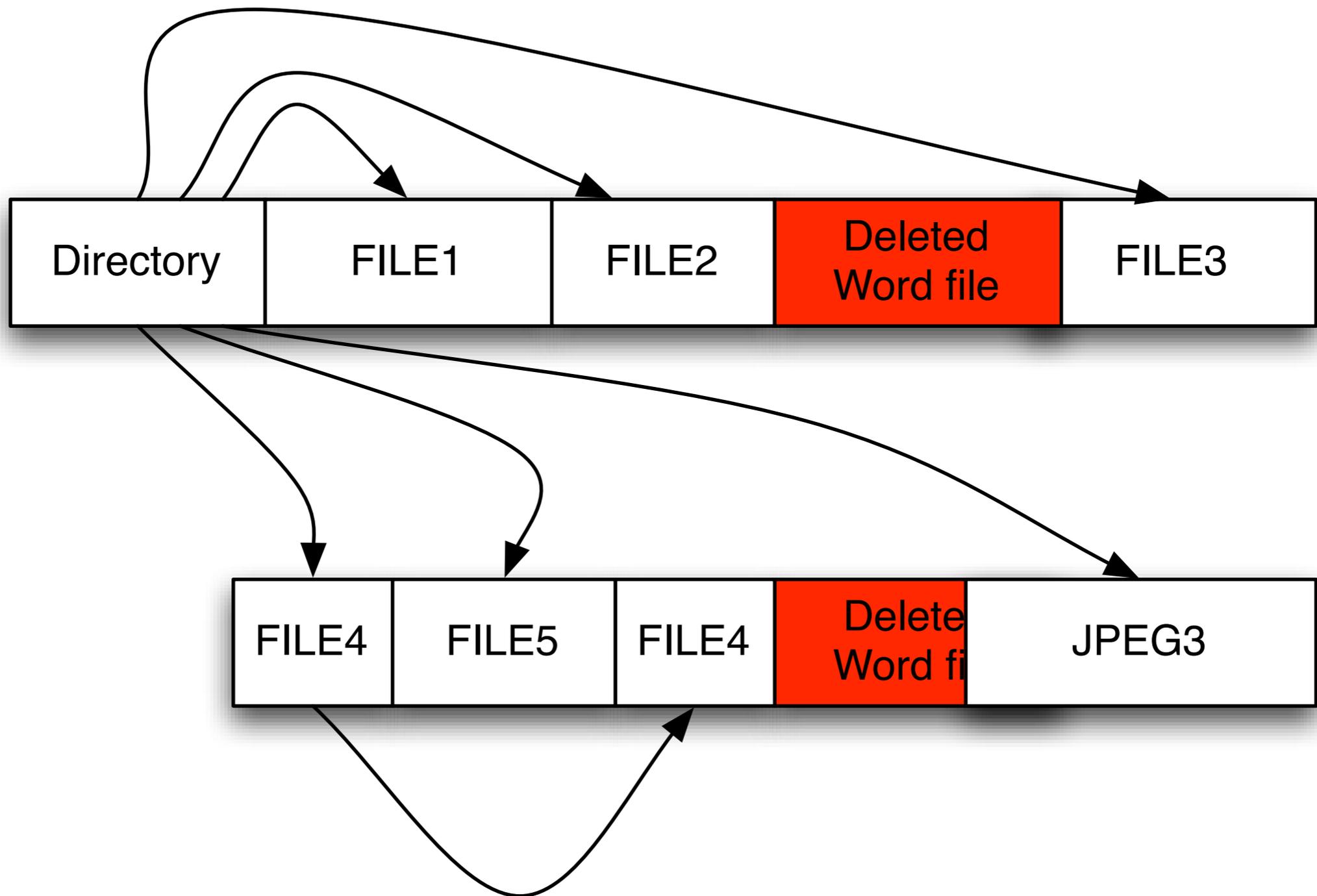
```
copy a:file.doc \dir
copy a:image.jpg \dir
del /dir/file.doc
copy a:mysong.mp3 \dir
```

Deleted files can be recovered because “delete” doesn’t really delete, it unlinks.



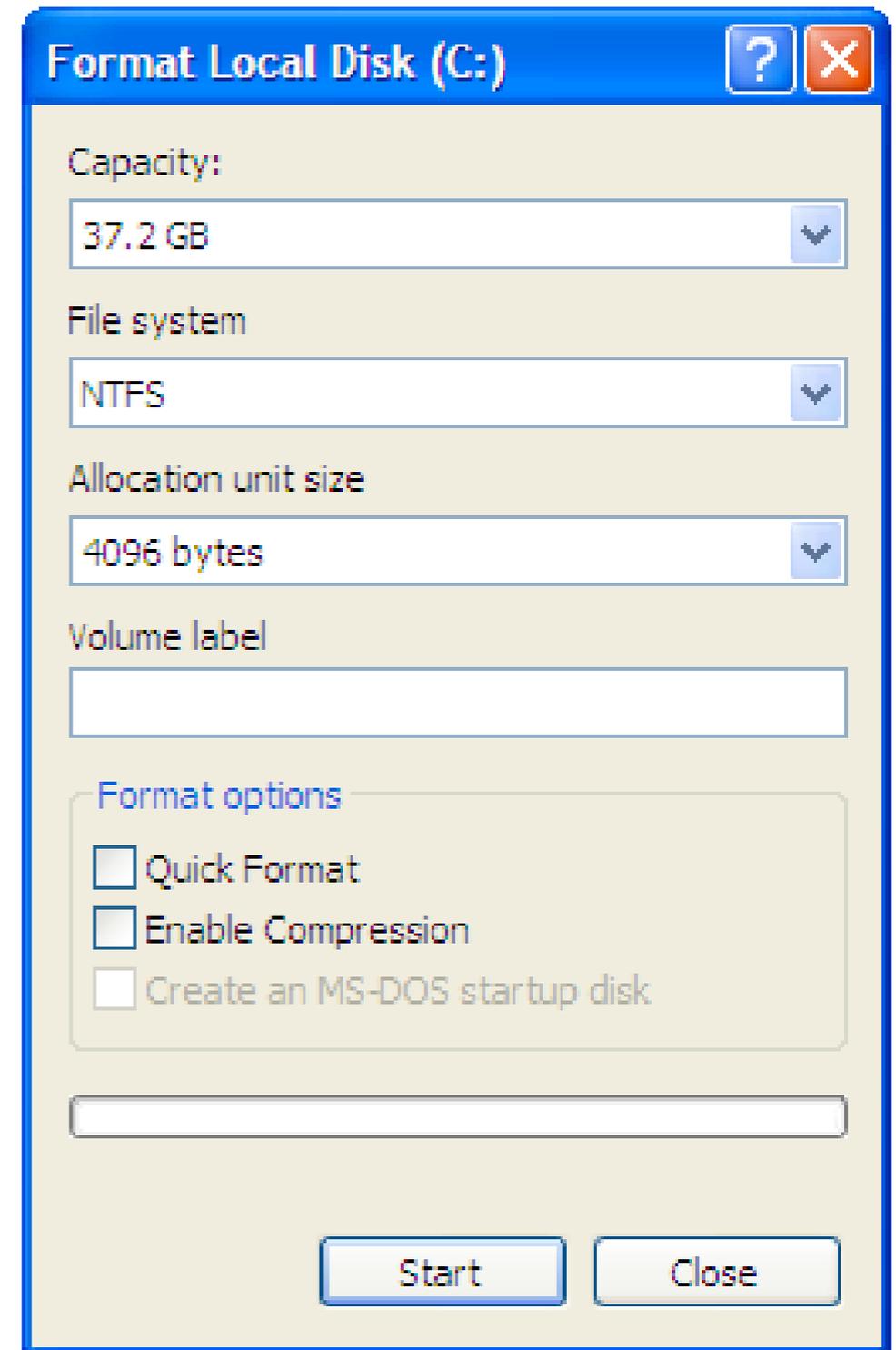
This is called “residual data”

As a result, a typical disk has many kinds of files and data segments on it:



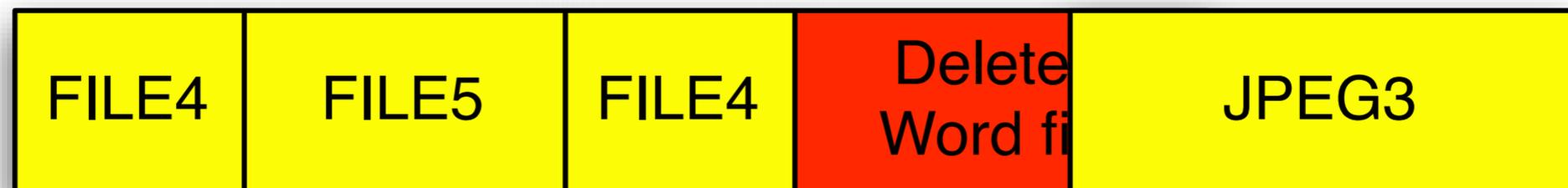
Formatting a disk just writes a new root directory.

```
C:\WINDOWS\system32\cmd.exe - format c:  
  
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)?
```



The image shows a Windows dialog box titled "Format Local Disk (C:)" with a blue title bar and standard window controls (help, close). The dialog is set to format the C: drive. It features several dropdown menus: "Capacity" is set to 37.2 GB, "File system" is set to NTFS, and "Allocation unit size" is set to 4096 bytes. There is an empty text field for "Volume label". Below these is a "Format options" section with three unchecked checkboxes: "Quick Format", "Enable Compression", and "Create an MS-DOS startup disk". At the bottom, there is a progress bar and two buttons: "Start" and "Close".

Formatting a disk just writes a new root directory.



There are many places that “deleted” information can hide

Free Space - Sectors on the “free list” (deleted but not overwritten)

Slack Space - Unused sectors at the end of an allocated cluster

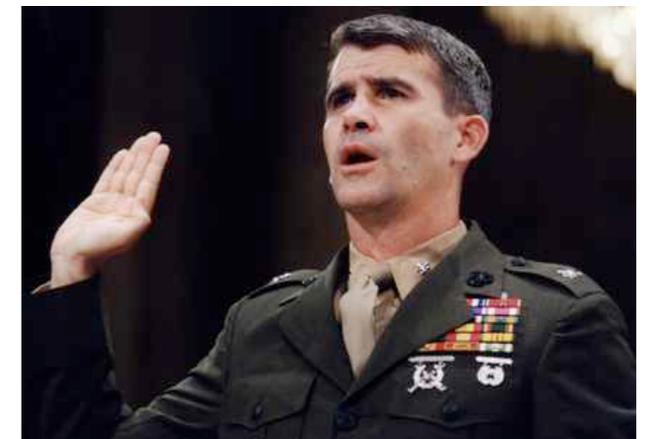
Cluster



Between partitions

Inside compound document files (MSOffice, etc.)

Backup Tapes



For more information, see:

“One Big File Is Not Enough: A Critical Evaluation of the Dominant Free-Space Sanitization Technique,” Garfinkel & Malan, PET 2006

Let's see what this looks like in practice.

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
```

Image this disk to a file,
then use the Unix “strings” command:

```
% strings 70.img | more
```

```
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 incompatible
```

```
version of Windows. Insert a Startup diskette matching this
```

```
OEMString = "NCR 14 inch Analog Color Display Enhanced SV
```

```
Graphics Mode: 640 x 480 at 72Hz vertical refresh.
```

```
XResolution = 640
```

```
YResolution = 480
```

% strings cont...

ling the Trial Edition

IBM AntiVirus Trial Edition is a full-function but time-limited evaluation version of the IBM AntiVirus Desktop Edition program. You may have received the Trial Edition on a promotional CD-ROM or as a single-file installation program over a network. The Trial Edition is available in seven national languages, and each language is provided on a separate CD-ROM or as a separate

EAS.STCm

EET.STC

ELR.STCq

ELS.STC

% strings 70.img cont...

MAB-DEDUCTIBLE

MAB-MOOP

MAB-MOOP-DED

METHIMAZOLE

INSULIN (HUMAN)

COUMARIN ANTICOAGULANTS

CARBAMATE DERIVATIVES

AMANTADINE

MANNITOL

MAPROTILINE

CARBAMAZEPINE

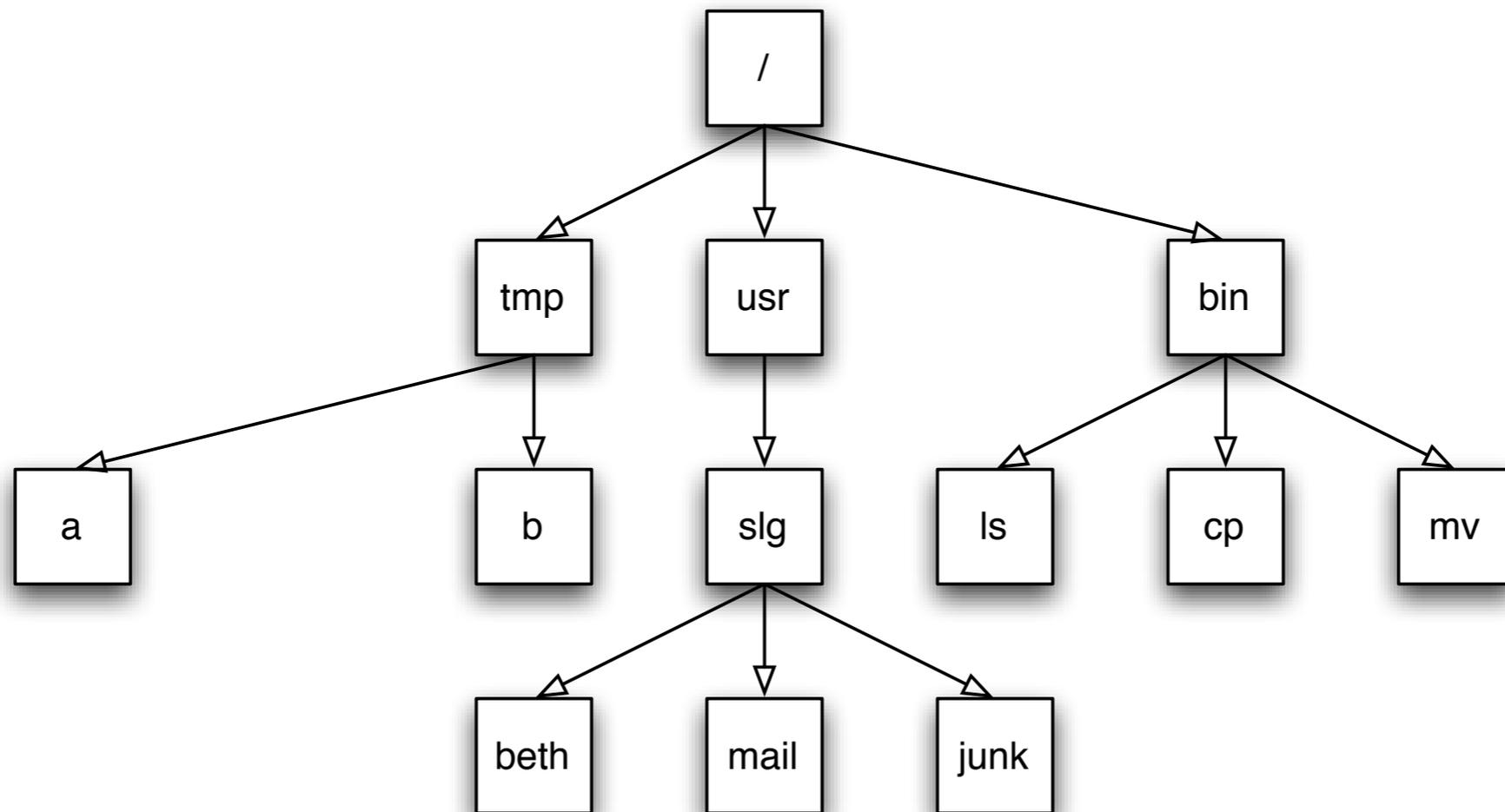
CHLORPHENESIN CARBAMATE

ETHINAMATE

FORMALDEHYDE

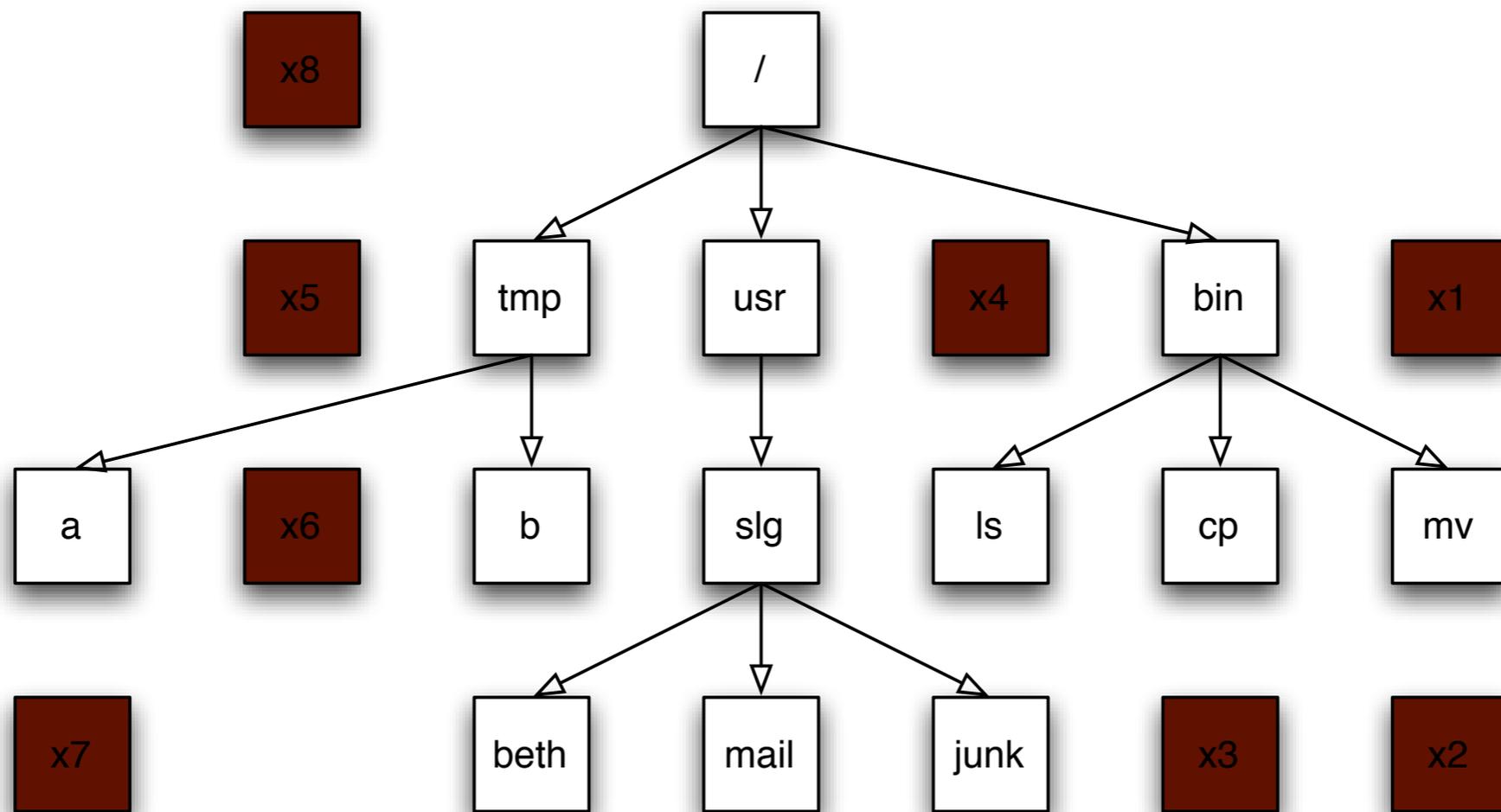
MAFENIDE ACETATE

Data on a hard drive is arranged in sectors



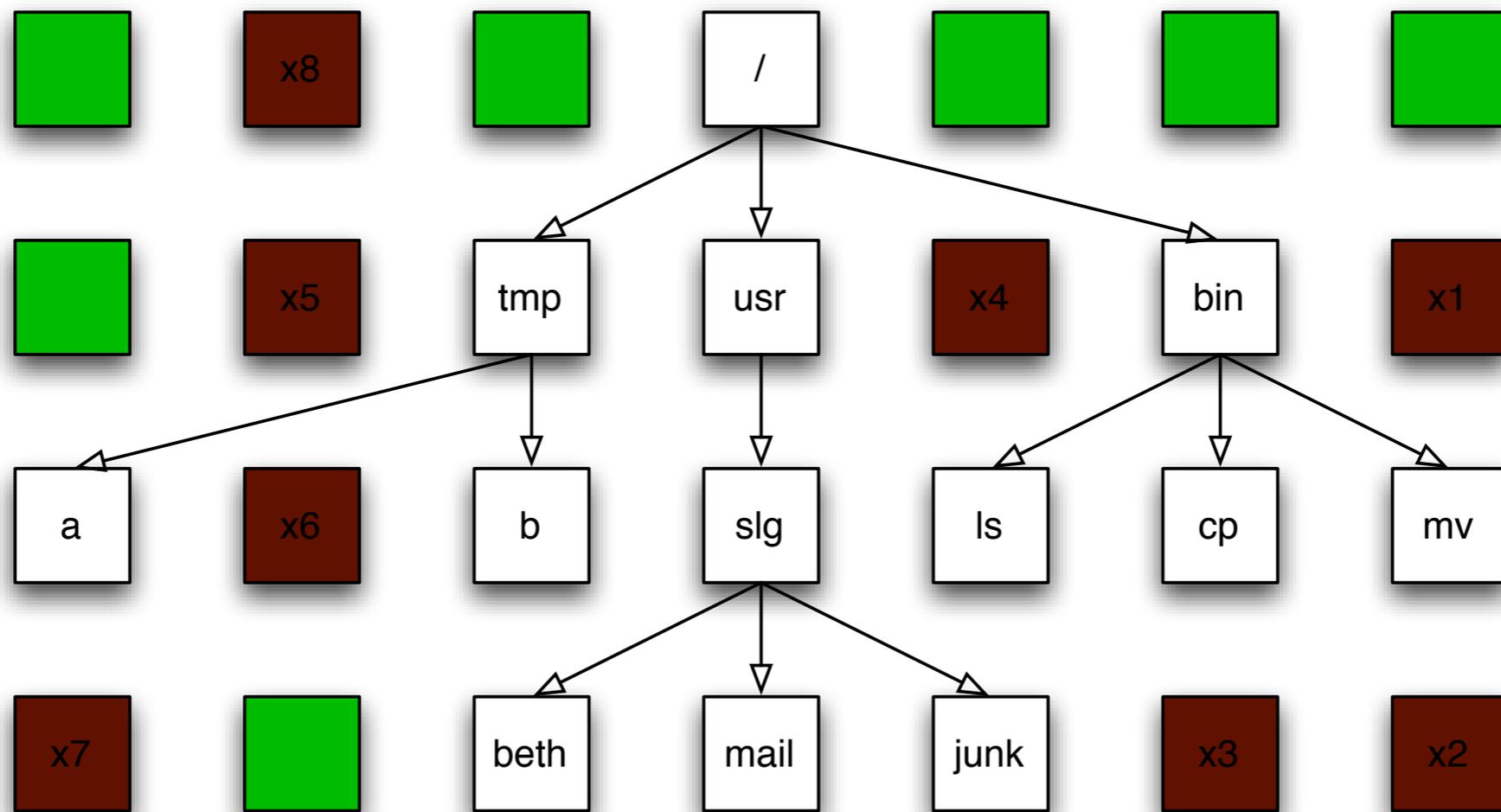
The white sectors indicate directories and files that are visible to the user

Data on a hard drive is arranged in sectors



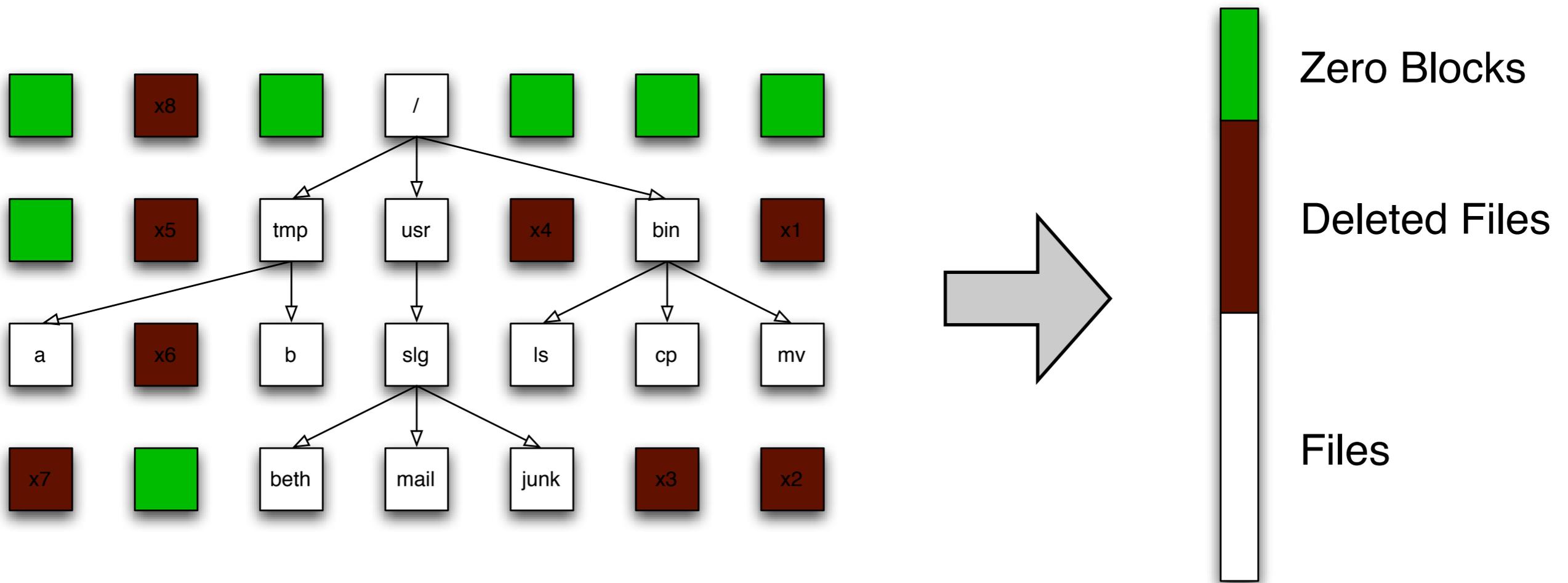
The brown sectors indicate files that were deleted.

Data on a hard drive is arranged in sectors

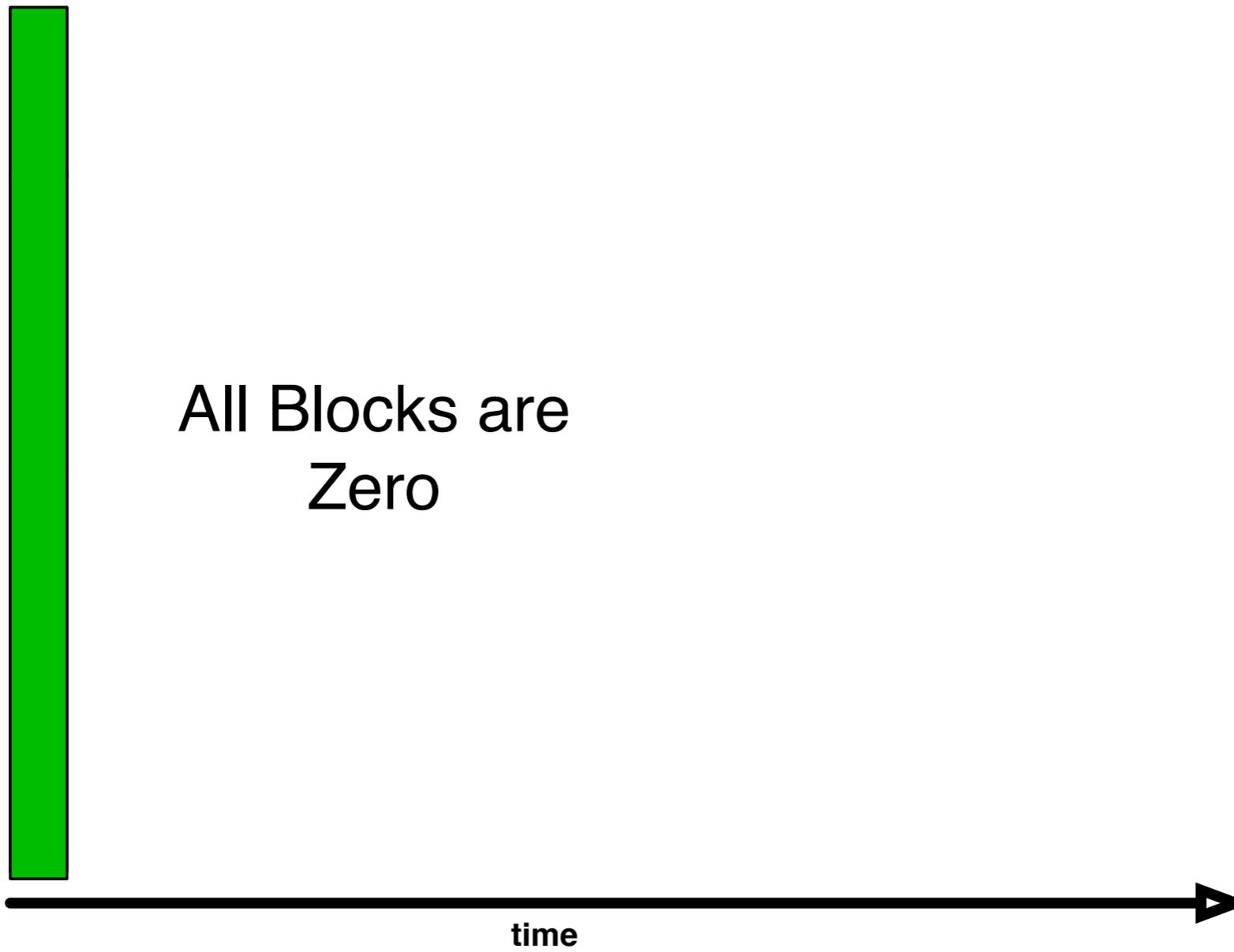


The green sectors indicate sectors that were never written (or that were wiped clean)

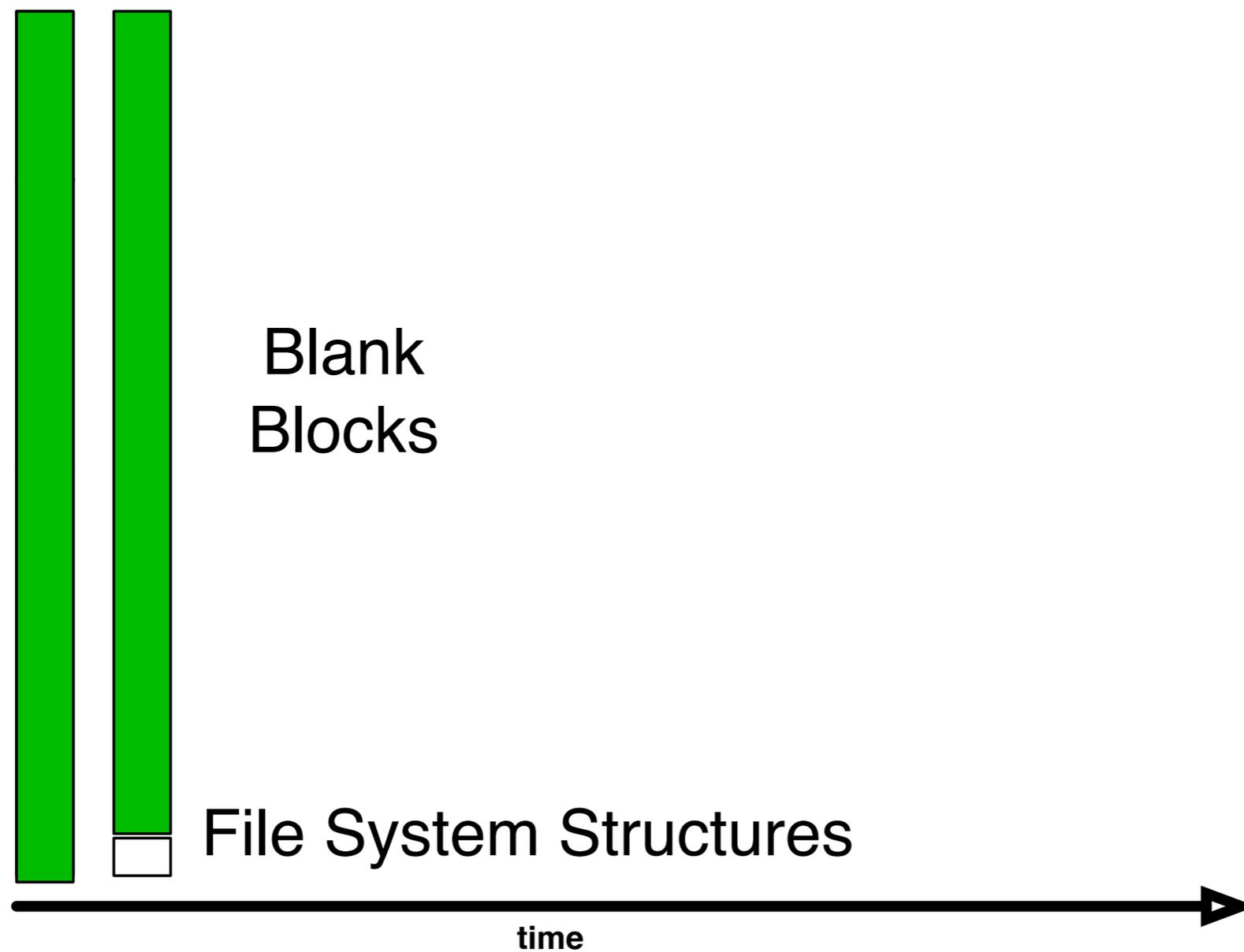
Stack the sectors:



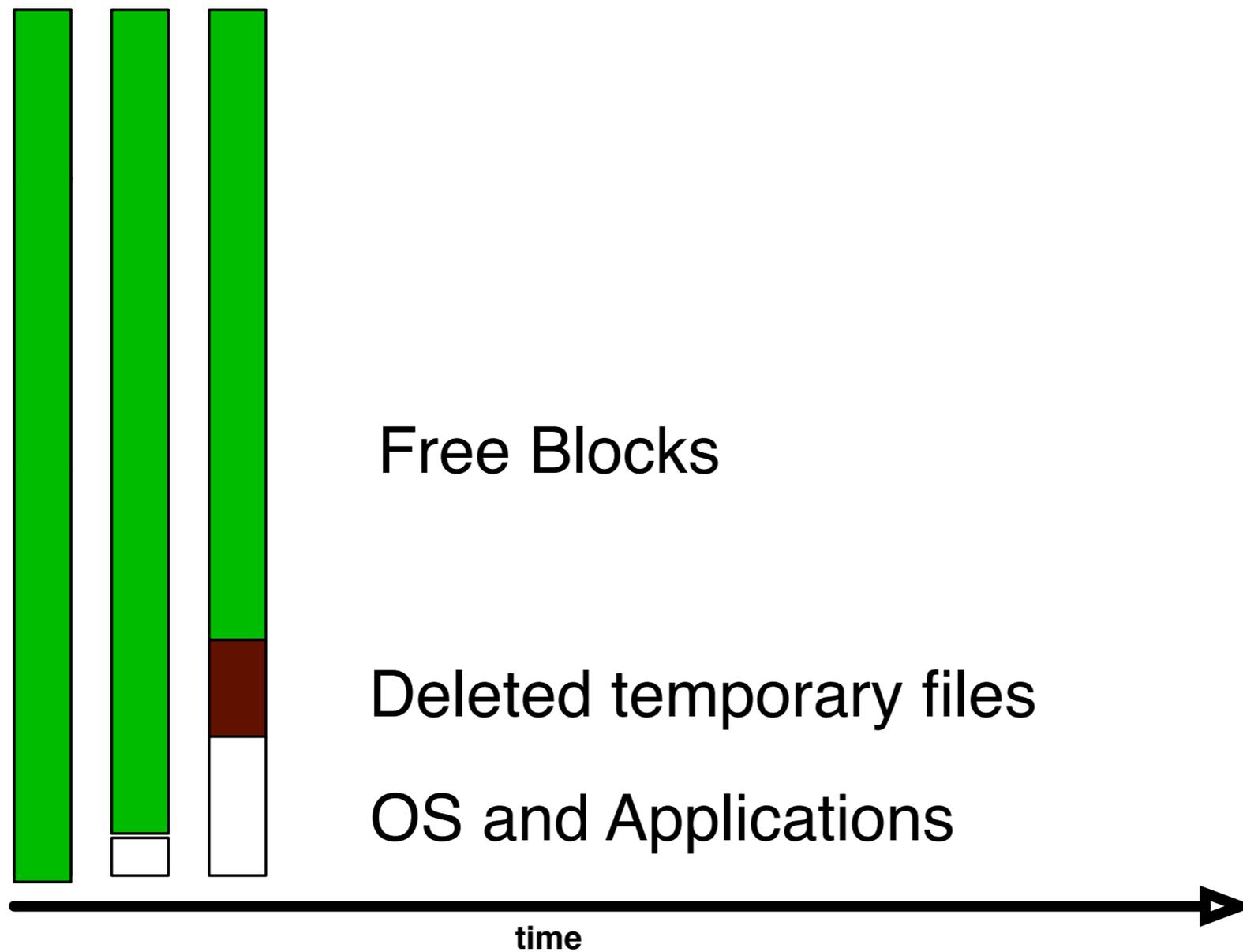
No data: The disk is factory fresh



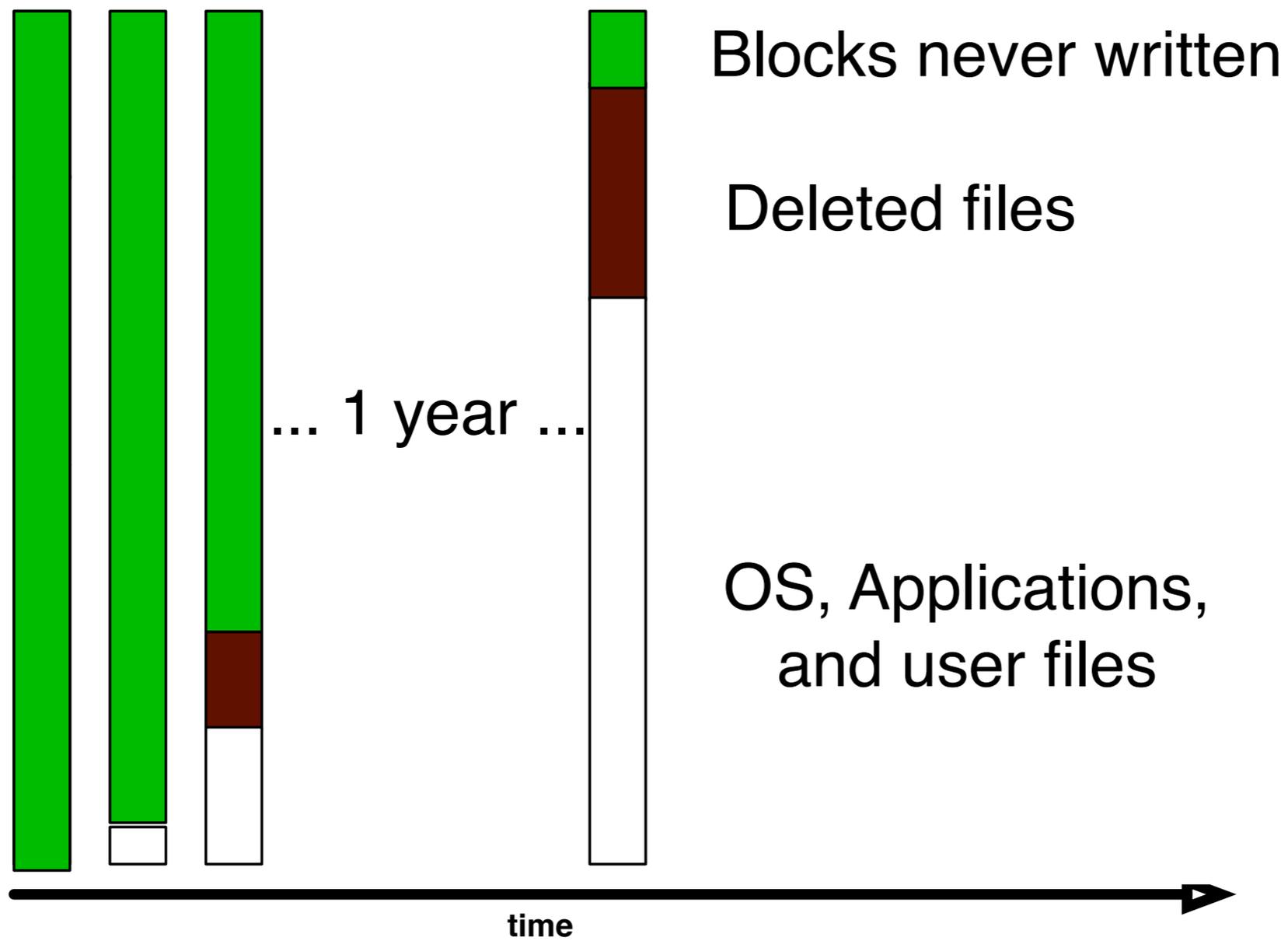
Formatted: the disk has an empty file system



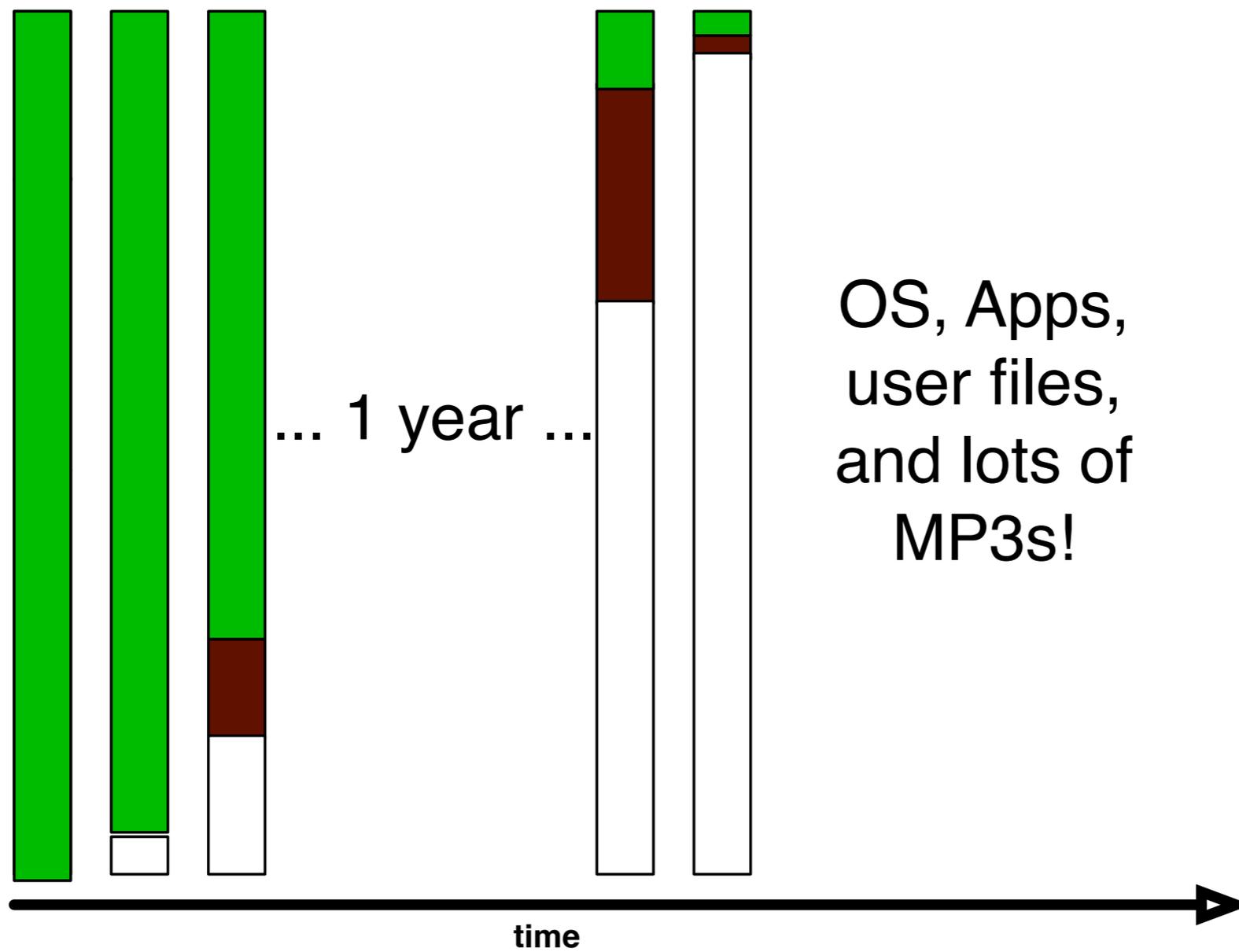
AFTER OS INSTALL: Temp. files have been deleted



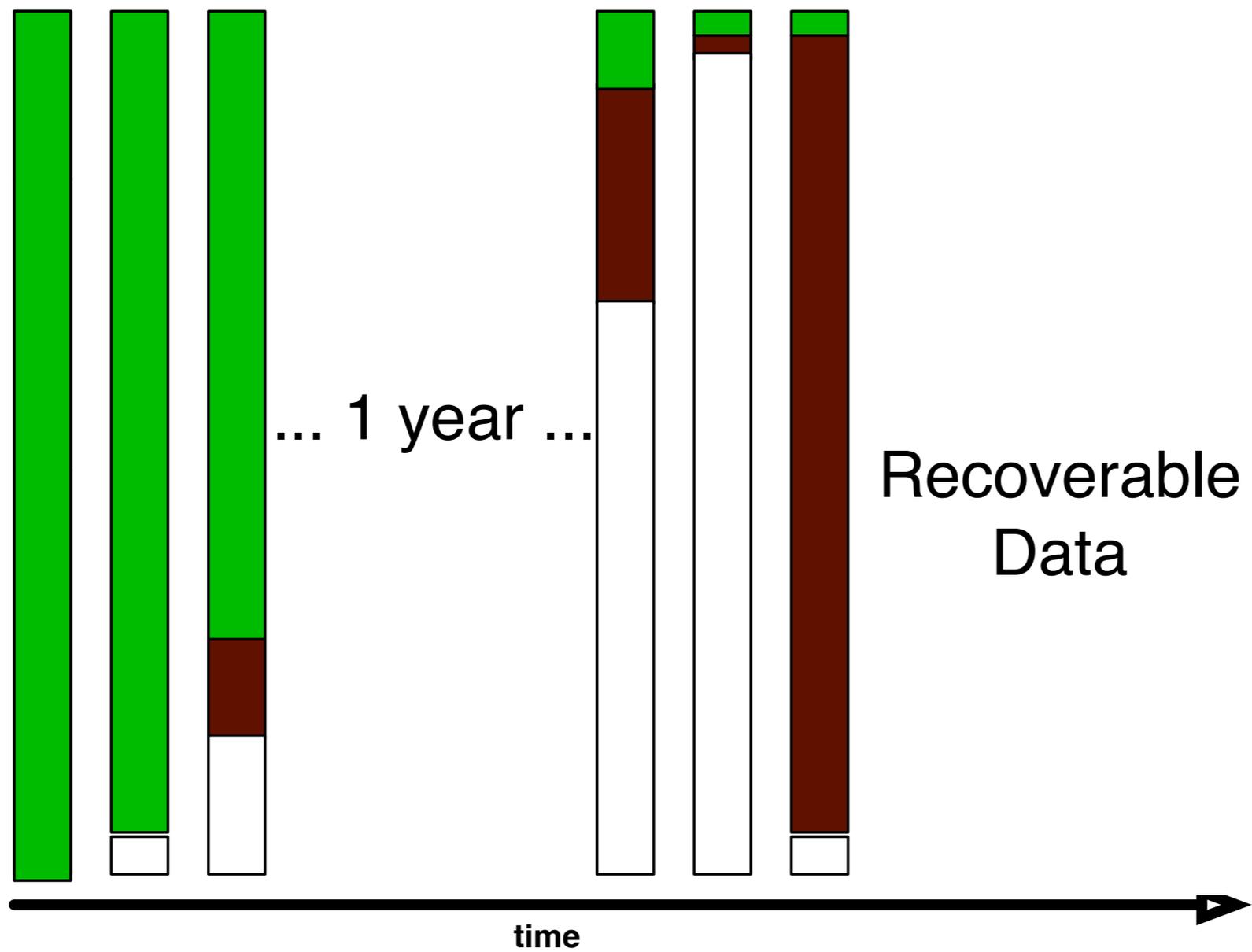
After a year of service



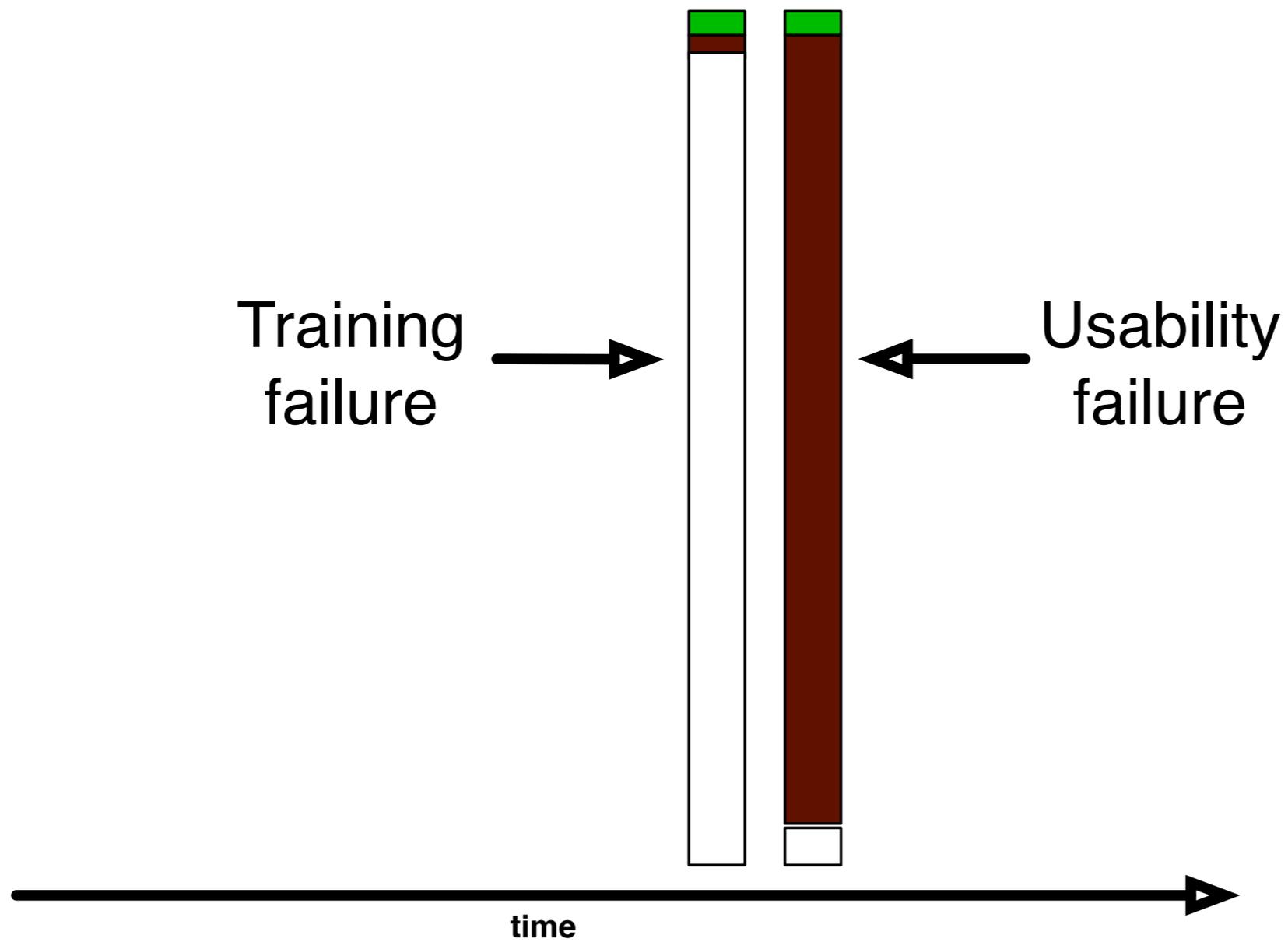
Disk nearly full!



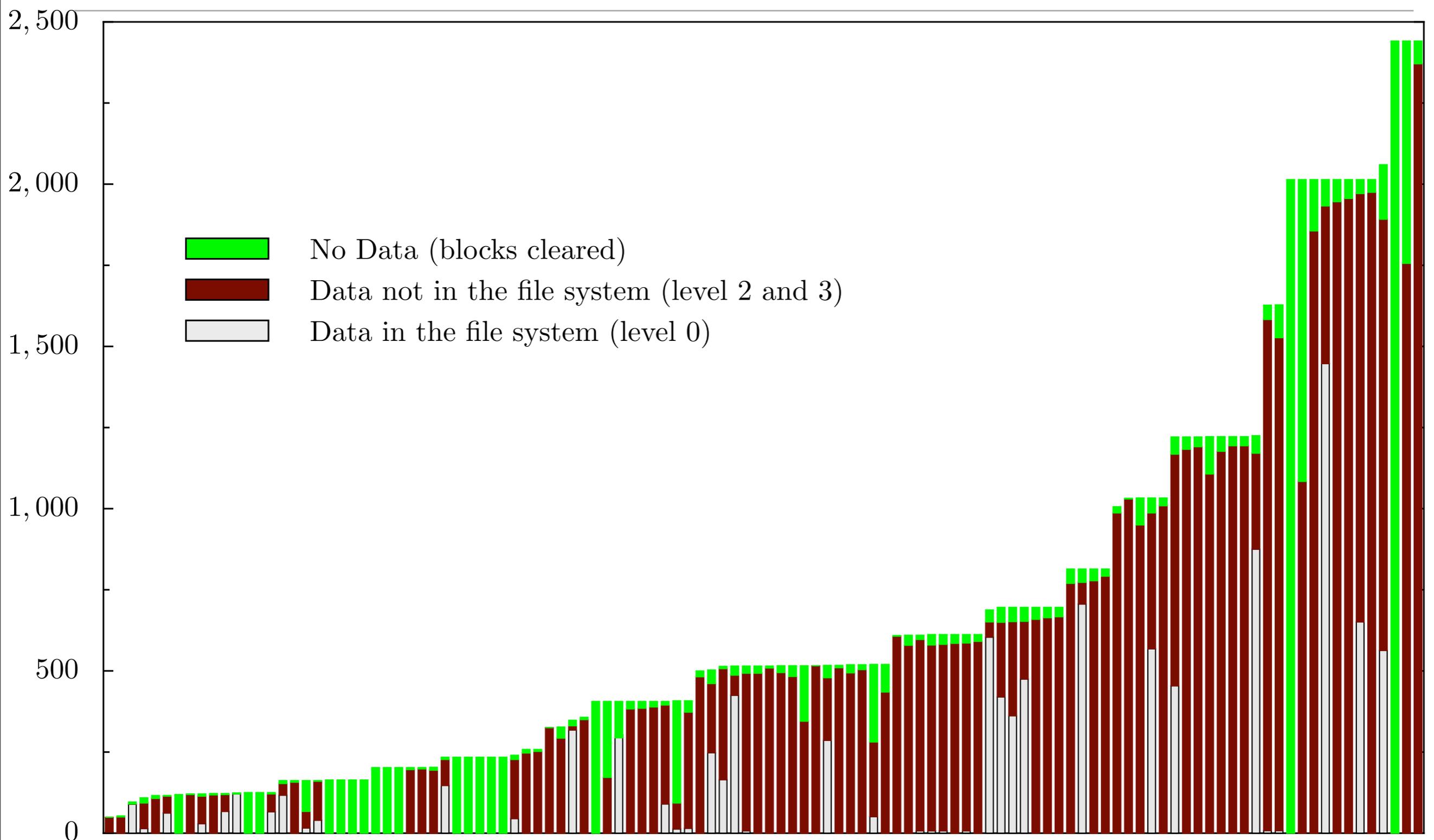
Let's sell the hard drive!
Format c:\



We can use forensics to reconstruct motivations:



Drives 1-236 are dominated by failed sanitization attempts.

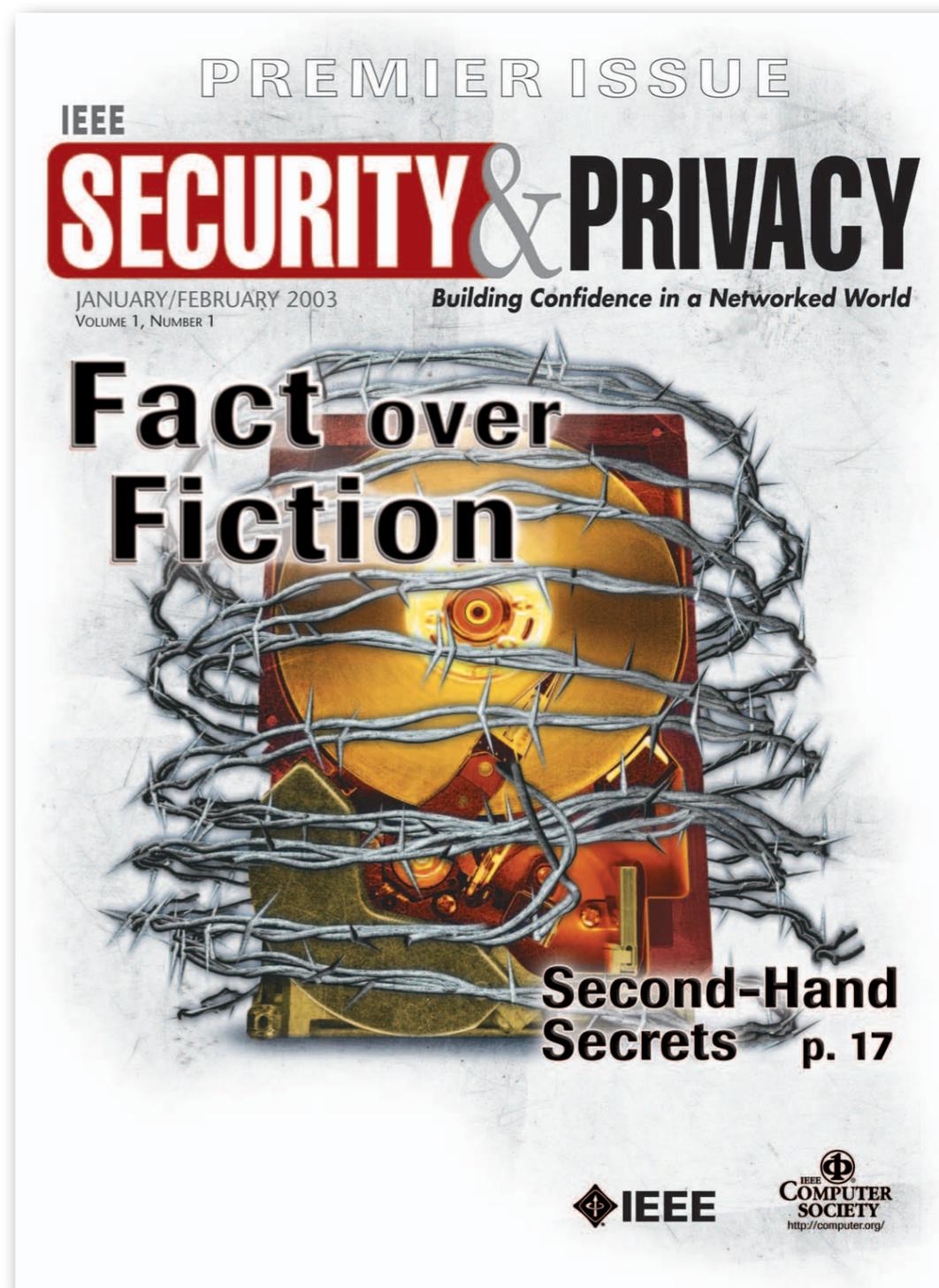


Roughly 1/3 of the discarded hard drives have significant amounts of confidential data.

From sampling 150 hard drives collected between 1998 and 2002, we found:

- Thousands of credit cards
- Financial records
- Medical information
- Trade secrets
- Highly personal information

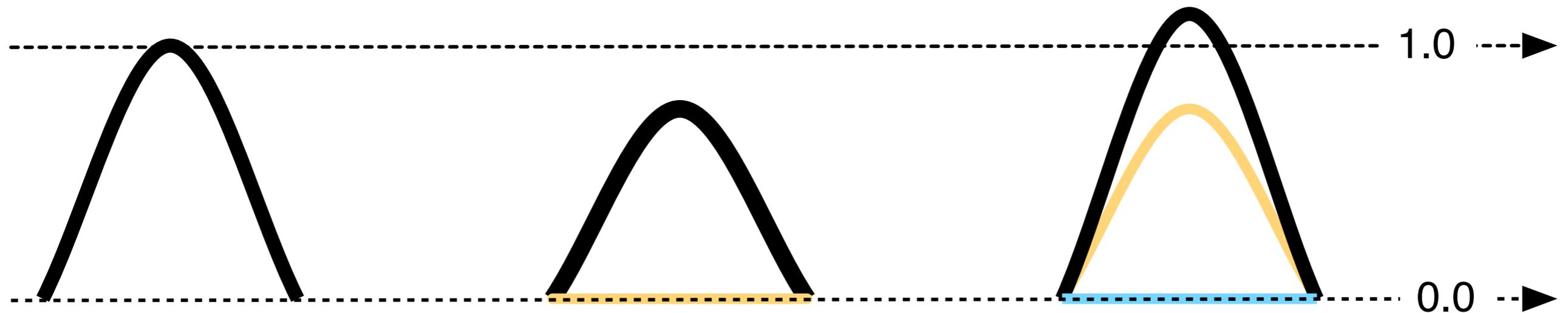
[Garfinkel & Shelat 03]



Question:

Can we recover data that's been overwritten?

Writing "1" over a "0" is different than writing a "0" over a "0"



Idealized "1"

"1" over a "0"

"1" over a "1"
over a "0"

This is called "remnant data"

DoD 5220.22-M Specifies a “sanitization” procedure for unclassified data

- Write a character
- Write its complement
- Write random data

In 1996 Peter Gutmann published a paper with 35 sanitization patterns.

srm defaults to a 7-pass pattern (F6, 00, FF, random, 00, FF, random)

Is the government trying to hide something from us?



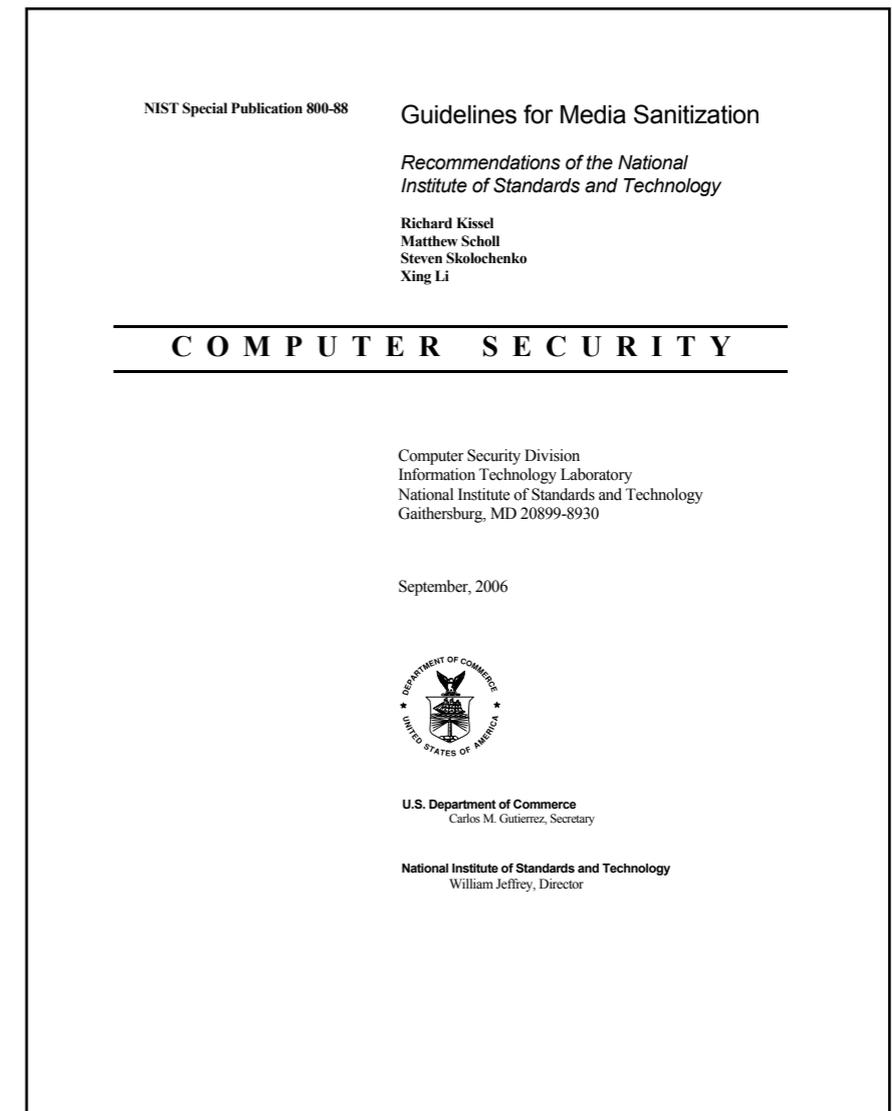
NIST states that it is very unlikely that overwritten data can be recovered.

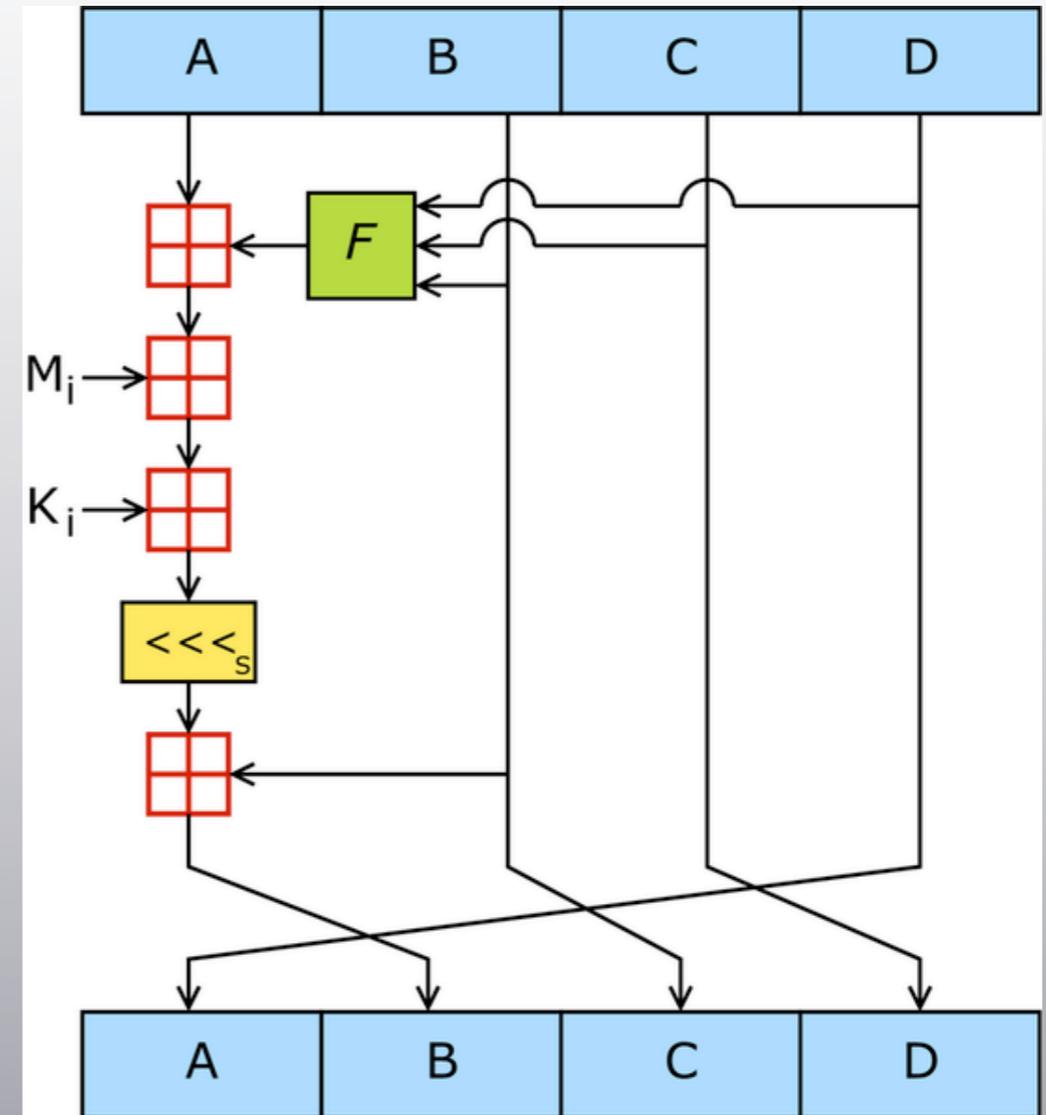
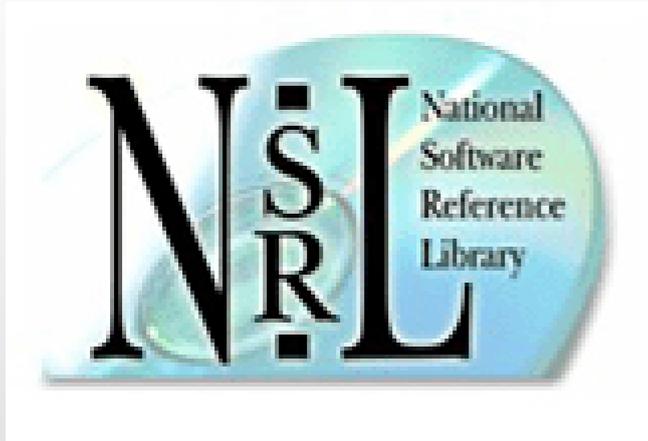
Modern disk drives are too complicated:

- Recording densities too high
- Use complex codes, not 0s & 1s
- No space between tracks
- Perpendicular recording will make things worse

It's never been demonstrated.

NIST 800-88, "Guidelines for Media Sanitization," says a single pass is good enough for ATA disks manufactured after 2001 (over 15GB).

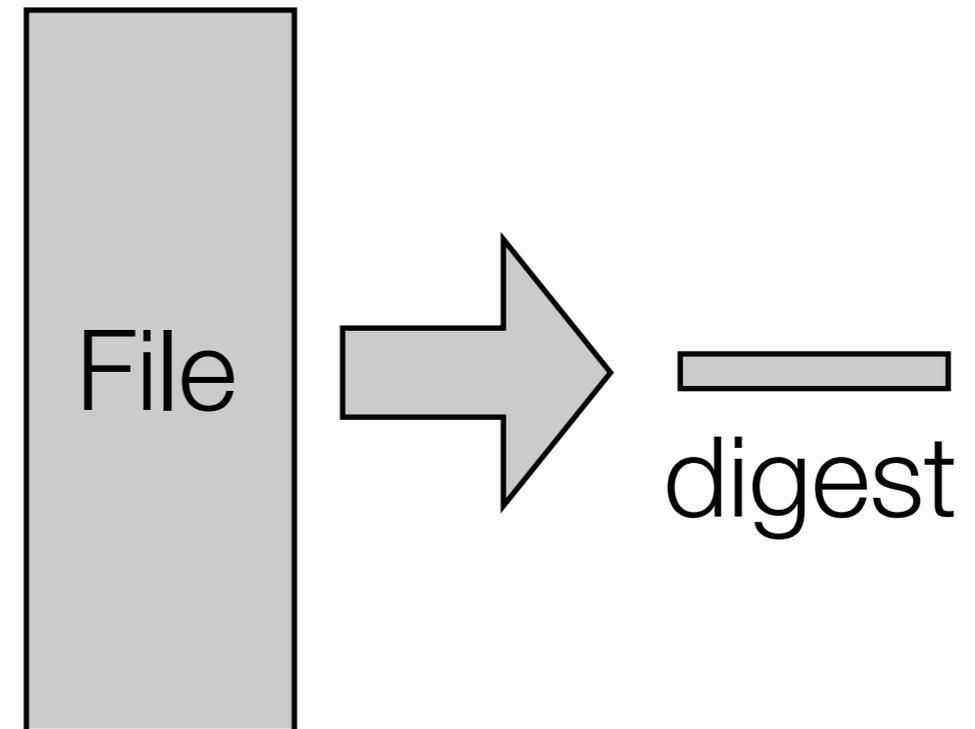




Understanding the National
Software Reference Library

Message Digests

1. Message Digests make a “fingerprint” of a file.
2. Input: 1-264 bytes
3. Output: 128 or 160* bits

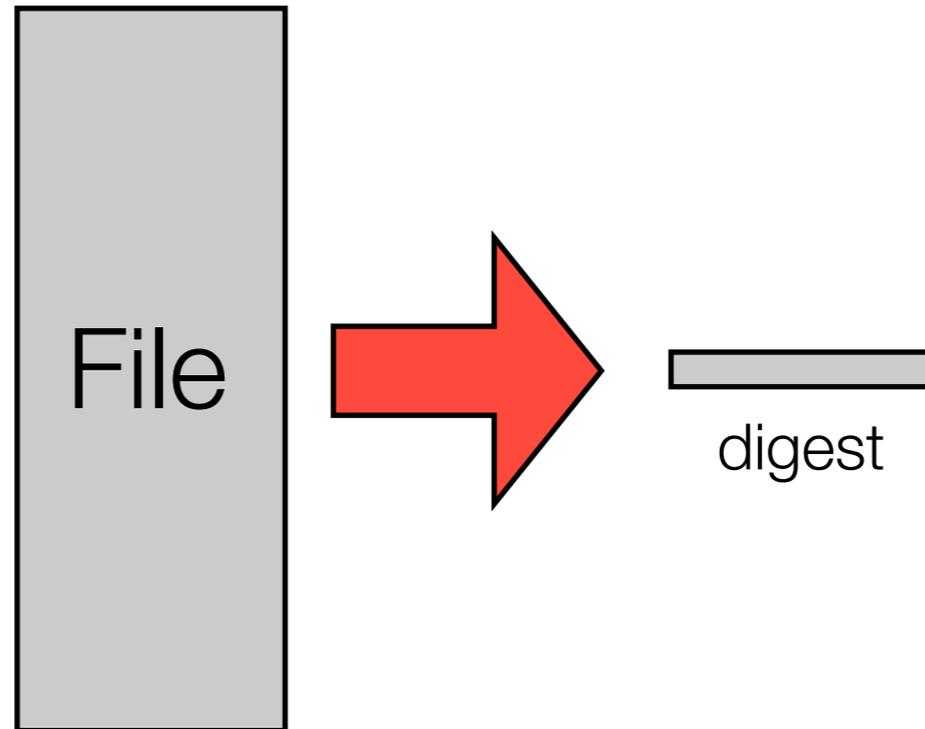


Message Digests

Message Digests make a “fingerprint” of a file.

Input: $1-2^{64}$ bytes

Output: 128 or 160^* bits

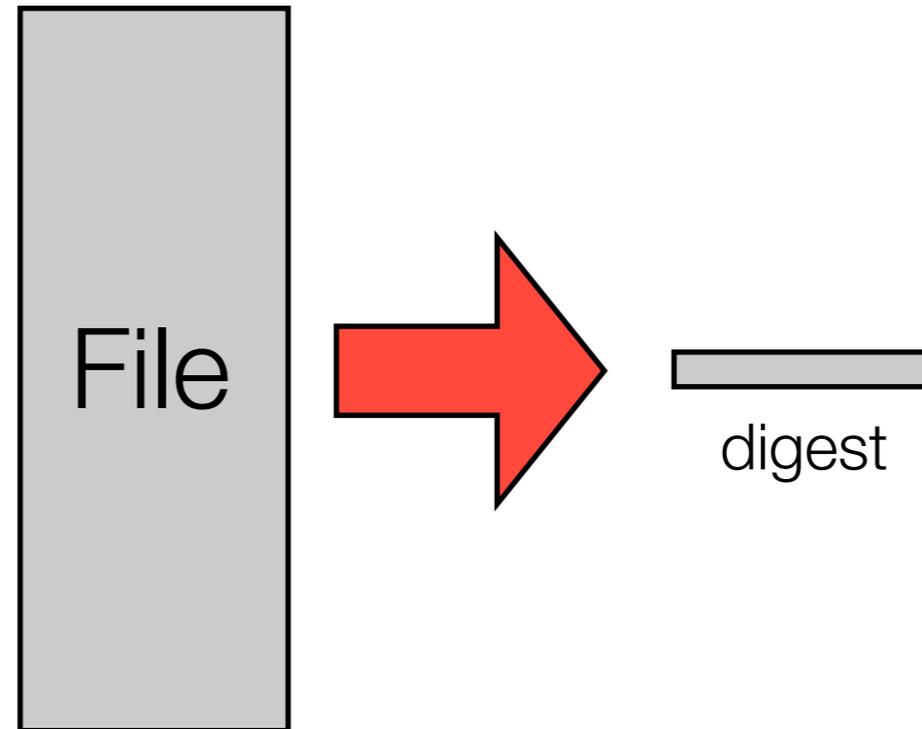


Message Digests

Message Digests make a “fingerprint” of a file.

Input: $1-2^{64}$ bytes

Output: 128 or 160* bits



Constitution of the United States of America
(In Convention, September 17, 1787)

Preamble

We the people of the United States, in order to form a more perfect union, establish justice, insure domestic tranquility, provide for the common defense, promote the general welfare, and secure the blessing of liberty to ourselves and our posterity, do ordain and establish the Constitution of the United States of America.

Article I.

Section 1. All legislative powers herein granted shall be vested in a Congress of the United States, which shall consist of a Senate and a House of Representatives.

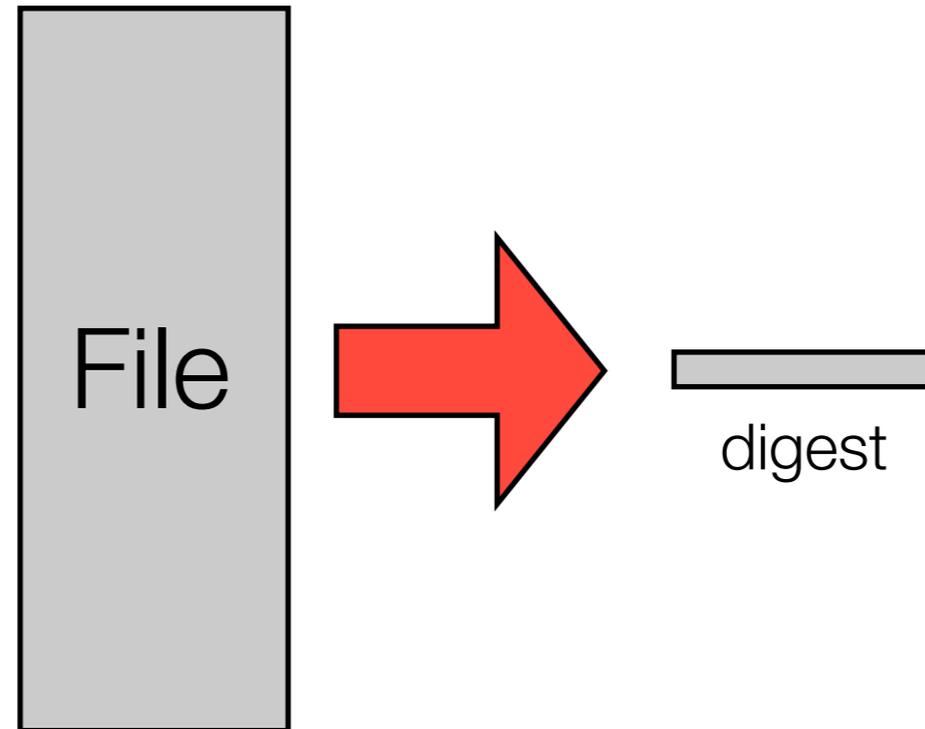
...

Message Digests

Message Digests make a “fingerprint” of a file.

Input: $1-2^{64}$ bytes

Output: 128 or 160^* bits



Constitution of the United States of America
(In Convention, September 17, 1787)

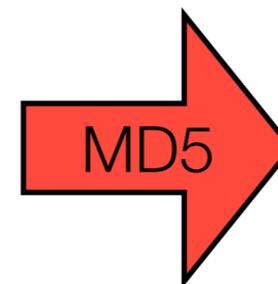
Preamble

We the people of the United States, in order to form a more perfect union, establish justice, insure domestic tranquility, provide for the common defense, promote the general welfare, and secure the blessing of liberty to ourselves and our posterity, do ordain and establish the Constitution of the United States of America.

Article I.

Section 1. All legislative powers herein granted shall be vested in a Congress of the United States, which shall consist of a Senate and a House of Representatives.

...

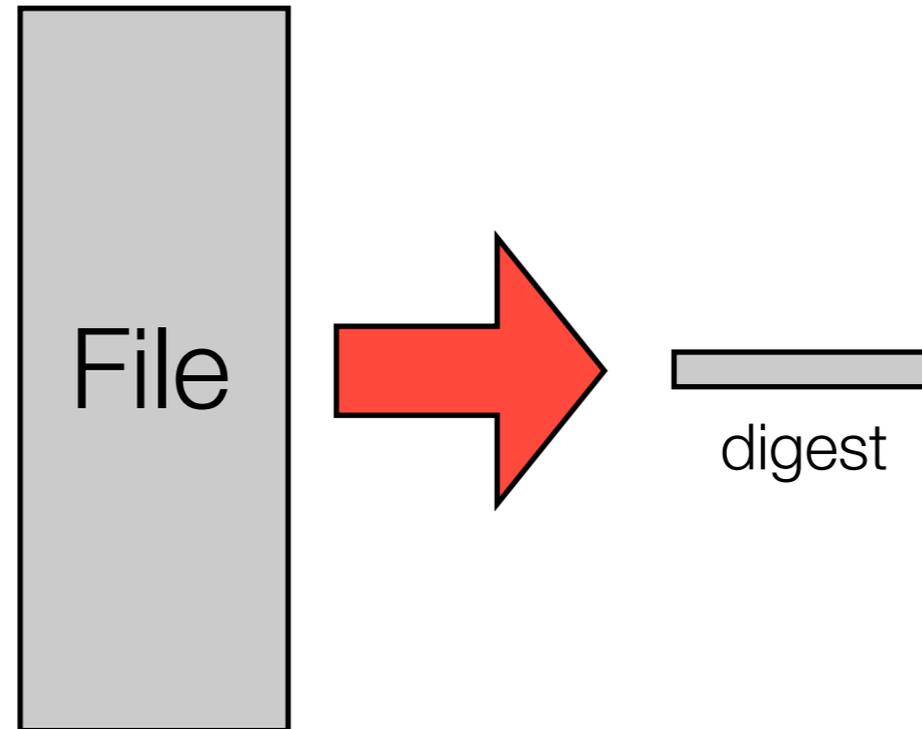


Message Digests

Message Digests make a “fingerprint” of a file.

Input: $1-2^{64}$ bytes

Output: 128 or 160^* bits



Constitution of the United States of America
(In Convention, September 17, 1787)

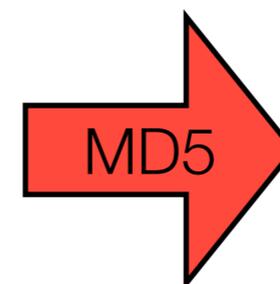
Preamble

We the people of the United States, in order to form a more perfect union, establish justice, insure domestic tranquility, provide for the common defense, promote the general welfare, and secure the blessing of liberty to ourselves and our posterity, do ordain and establish the Constitution of the United States of America.

Article I.

Section 1. All legislative powers herein granted shall be vested in a Congress of the United States, which shall consist of a Senate and a House of Representatives.

...



`bab1c005bad1ac7
d58d54d0e5d0e5f3f`

Properties of a good Message Digest

$$\text{Digest} = f(\text{Input})$$

1. Digest cannot be predicted from the input
2. Hard or impossible to find two inputs with the same digest.
3. Changing one bit of input changes ~50% of the output bits.

Message Digest Algorithms

Rivest Functions:

- MD2 (RFC 1319), MD4 (RFC 1320), MD5 (RFC 1321)

NIST Functions:

- SHA, SHA-1, SHA-512, SHA-1024

Other Functions:

- Snerfu, N-Hash, RIPE-MD, HAVAL

Message Digest Example

message	MD5(message)
“this is a test”	ff22941336956098 ae9a564289d1bf1b
“this is c test”	c5e530b91f5f324b 1e64d3ee7a21d573
“this is a test ”	6df4c47dba4b01cc f4b5e0d9a7b8d925

Key Points about hash functions:

Any change in the input usually changes the digest:

- Adding a space
- Changing a line break
- Capitalizing a word

It's computationally difficult to:

- Find two inputs that have the same hash
- Create an input to match a given hash
- Change an input without changing the hash

“Breaking” a message digest

Brute-force attack:

- Search for two messages that have the same digest (they should be many of them)
- Create a message with a desired message digest

Algorithm attack

- Using your knowledge of match, create two document with a given digest.

The National Software Reference Library is an official list of hash values.

4 CDROMs:

- A - non-English software
- B - operating systems
- C - applications
- D - images

Each CDROM has 5 files:

- NSRFile.txt - List of hashes (SHA-1 & MD5), file names, & products
- File.txt-md5.idx - Sorted hash codes, with index offset
- NSRlMfg.txt - Manufacturer codes
- NSRLOS.txt - Operating system codes
- NSRlProd.txt - Product codes

NSRFile.txt:

```
"SHA-1", "MD5", "CRC32", "FileName", "FileSize", "ProductCode", "OpSystemCode", "SpecialCode"  
"00000142988AFA836117B1B572FAE4713F200567",  
  "9B3702B0E788C6D62996392FE3C9786A", "05E566DF", "J0180794.JPG", 32768, 2322, "WIN", ""  
"00000142988AFA836117B1B572FAE4713F200567",  
  "9B3702B0E788C6D62996392FE3C9786A", "05E566DF", "J0180794.JPG", 32768, 3271, "WIN", ""  
"00000142988AFA836117B1B572FAE4713F200567",  
  "9B3702B0E788C6D62996392FE3C9786A", "05E566DF", "J0180794.JPG", 32768, 3290, "WIN", ""  
"000005EE5E3F6961B78CE4549270DE5D05CBC0CB",  
  "8D025B6AE1994A40FCBB5AEC2EF273F9", "5E8D7D42", "WabIab.bor", 4760, 4616, "WIN", ""  
"0000085FC602CD8AD4793A874A47D286DACB0F6A",  
  "8BA8BC04896C421A704282E9B87B5520", "8D89A85D", "fpSDtFindLink.gif",  
1161, 2988, "Solaris", ""  
"00000FF9D0ED9A6B53BC6A9364C07074DE1565F3",  
  "A5D49D6DA9D78FD1E7C32D58BC7A46FB", "2D729A1E", "cmnres.pdb.dll", 76800, 1550, "WIN", ""  
"00000FF9D0ED9A6B53BC6A9364C07074DE1565F3",  
  "A5D49D6DA9D78FD1E7C32D58BC7A46FB", "2D729A1E", "cmnres.pdb.dll", 76800, 2704, "WIN", ""
```

NSRLEFile.txt-md5.idx

```
0000000000000000000000000000000000000000000000000000000000000000 | nsrl
00000238B43AF52EB6F9780D25173C | 0000000407470726
00000B3A8ABFCD7F061689833A1BA01F | 0000001219208863
00000C9D411182EBCD58AF5AC7278E23 | 0000000371257953
000016F07018F95BF4B01E7E11583484 | 0000000835645085
00001FE023957C19D5E70FA34085B623 | 0000000935899154
0000222286FAC25C704D56A6B3831128 | 0000000885465166
0000224DF8086F79200CADED083A7F8F | 0000000988385431
00002C6A13B13FB588B87C6204E73B0C | 0000000134913247
0000315467D336EB5EF32C584AEA63EC | 0000000160461562
00003EB4947FBFBD8A0BE1CDD7627A69 | 0000001214903627
00003F1384170EA6E1990A16AC95DF06 | 0000001072802295
00004343D9902EC1BC85EA30BE0F1FE8 | 0000000278826509
000049127C704B1439A71903B0957D0B | 0000001044376928
00004D6B90025BB8D41F1DD5D3CF4883 | 0000000013716287
00005B410A87A2AC4925DDDF96EA5FAF | 0000000929906503
000062D41CD86146968F0FD6215645DB | 0000001084349301
0000639B16A7D98B4FA66DB1E01D46A0 | 0000000341249091
000069C2686A95F5B334A36ECEBAEC42 | 0000000894786950
00006DA40DC2DCBE0AD5305236B21F00 | 0000000749097504
0000761515A867A4AF658D268F2F1B39 | 0000001043646298
```

NSRLOS.txt

```
"AIX", "AIX", "Generic", "Unknown"  
"AIX43", "AIX 4.3", "4.3", "IBM"  
"AIX432", "AIX 4.3.2", "4.3.2", "IBM"  
"AIX433", "AIX 4.3.3", "NA", "Unknown"  
"AIX51", "AIX 5.1", "5.1", "IBM"  
"AS/400", "AS/400", "N/A", "Unknown"  
"AT", "AT", "NA", "Unknown"  
"AT&T", "AT&T", "Unknown", "AT&T"  
"Amiga", "Amiga", "Unknown", "Unknown"  
"Amstrad_6128", "Amstrad 6128", "Unknown", "Unknown"  
"Apple Iic", "Apple IIC", "Unknown", "Apple"  
"Apple_II+", "Apple II+", "Unknown", "Apple"  
"Apple_IIGS", "Apple IIGS", "Unknown", "Apple"  
"Apple_IIE", "Apple IIE", "Unknown", "Apple"  
"Atari_ST", "Atari ST", "Unknown", "Unknown"  
"CE", "CE", "Unknown", "Microsoft"  
"CommodoreAmiga", "Commodore Amiga", "Unknown", "Unknown"  
"Commodore_64", "Commodore 64", "Unknown", "Unknown"
```

How to use NSRL

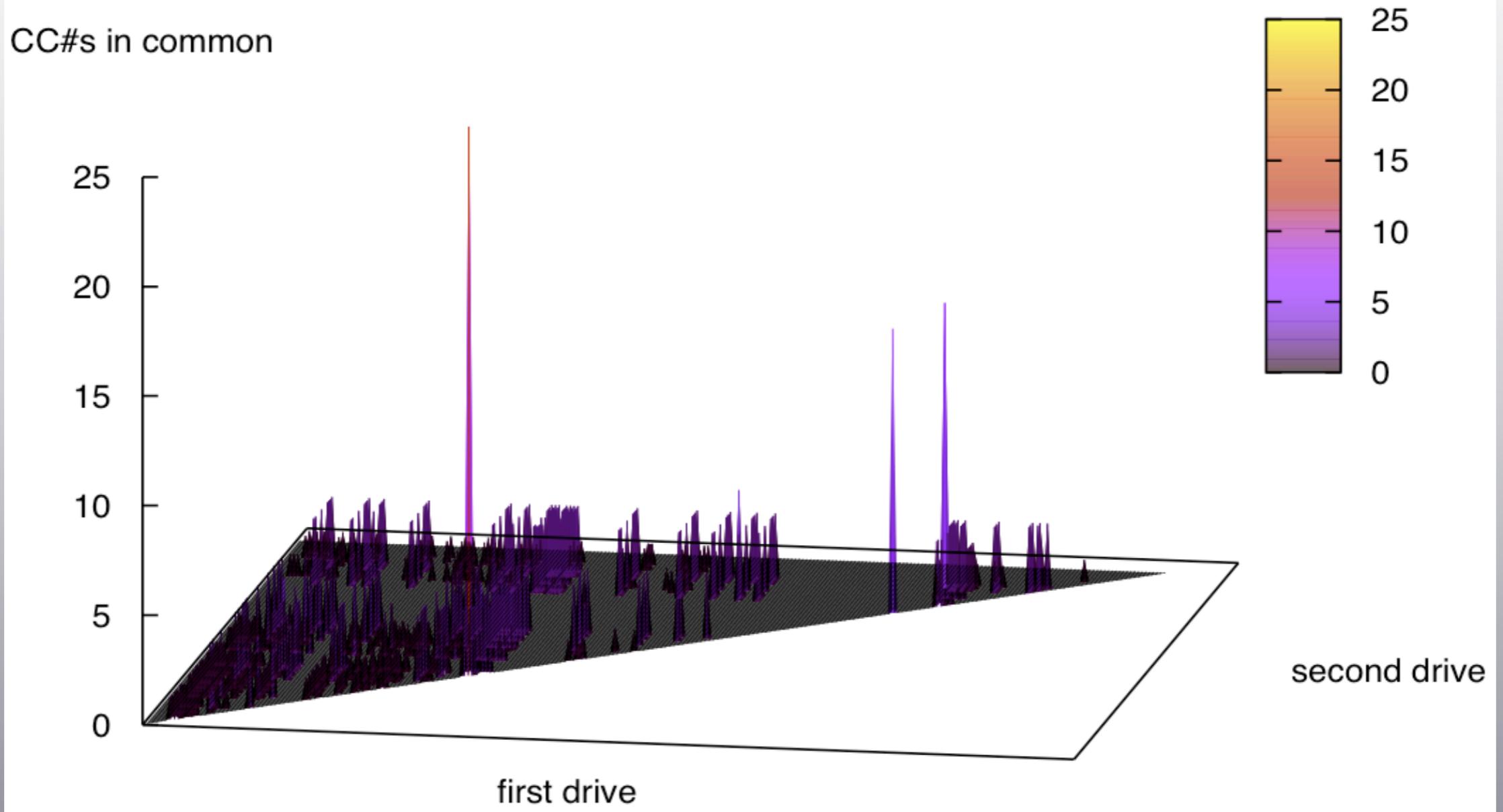
You can subscribe to get the current version.

Or you can download ISOs of older versions from the NSRL website.

NSRL can be used by most computer forensic tools...

... or write your own tools!

Cross Drive Correlation

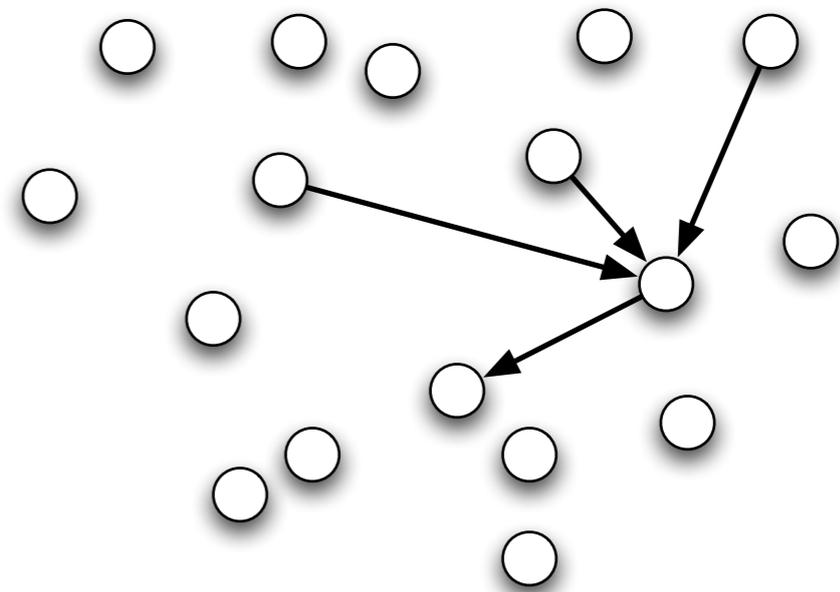


Cross-Drive Analysis

Cross-Drive Analysis is a tool for correlating pseudo-unique information across disk drives

Uses of cross-drive analysis:

- Identifying drive owner.
- Finding social networks
- Scoring probability of inclusion in a network.



A “feature” is any kind of pseudo-unique information

Credit Card Number (CCN)

XXXX-YYYY-ZZZZ-QQQQ or XXXXYYYYZZZZQQQQ

“XXXX” is a well-known prefix.

validate(“XXXXYYYYZZZZQQQQ”) is true

Email addresses

e.g. user@company.com

RFC-822 Time and Message-ID detector

<Pine.LNX.4.61.0705090002250.6378@conundrum.infosecnews.org>

Date: Wed, 9 May 2007 00:02:51 -0500 (CDT)

Internet Explorer cache, cookies, etc.

CCN Detector: written in flex and C++

Disk #105:

Test	# pass
pattern	3857
Known prefixes	90
CCV1	43
patterns & histogram	38

Sample output:

```
' CHASE NA | 5422-4128-3008-3685 | pos=13152133
' DISCOVER | 6011-0052-8056-4504 | pos=13152440
. ' GE CARD | 4055-9000-0378-1959 | pos=13152589
BANK ONE | 4332-2213-0038-0832 | pos=13152740
. ' NORWEST | 4829-0000-4102-9233 | pos=13153182
' SNB CARD | 5419-7213-0101-3624 | pos=13153332
```

Occasional false positives are largely irrelevant.

Disk #115:

Test	# pass
pattern	9196
Known prefixes	898
CCV1	29
patterns & histogram	13

Sample output:

```
.....@: | 44444486666108 | :<@<74444:@@@<<44 pos=82473275
.....#"&'&&' | 445447667667667 | ..050014&'4"1"&' . pos=86493675
.....221267241667& | 454676676654450 | &566746566726322. pos=86507818
3..30210212676677.. | 30232676630232 | .1.....001.01 pos=86516059
"&#&&'&41&&'645445& | 454454672676632 | .3.....0.. pos=86523223
....." .#"#"#&' | 445467667227023 | .....366 pos=87540819
D#9?.32400.,,+14%?B | 499745255278101 | *02)46+;<17756669 pos=118912826
.GGJJB...>.JJGG...G | 3534554333511116 | .....6 pos=197711868
%.....}}}}}}..... | 44444322233345 | .....}}}}}}..... pos=228610295
%6"! ) .&*%,,%-0)07. | 373484553420378 | <67<038+.5(+0+.3. pos=638491849
%6"! ) .&*%,,%-0)07. | 373484553420378 | <67<038+.5(+0+.3. pos=645913801
```

Results of scanning the 2003 corpus with CCN scanner:

Total number of image files:	178
Number of CCNs found:	47,771
Number of distinct CCNs:	15,613
Most popular CCN:	6404 6521 6029 6650 (34 times on 30 drives)

Context analysis shows this is not a valid CCN:

```
[6] 6213 1 6758 6367 .. | 6404 6521 6029 6650 | v 6025 6646 1 -138
[7] 6213 1 6758 6367 .. | 6404 6521 6029 6650 | v 6025 6646 1 -138
[8] 6213 1 6758 6367 .. | 6404 6521 6029 6650 | v 6025 6646 1 -138
[10] 6213 1 6758 6367 .. | 6404 6521 6029 6650 | v 6025 6646 1 -138
[11] 6213 1 6758 6367 .. | 6404 6521 6029 6650 | v 6025 6646 1 -138
[11] 6213 1 6758 6367 .. | 6404 6521 6029 6650 | v 6025 6646 1 -138
[15] 6213 1 6758 6367 .. | 6404 6521 6029 6650 | v 6025 6646 1 -138
[18] 6213 1 6758 6367 .. | 6404 6521 6029 6650 | v 6025 6646 1 -138
[18] 6213 1 6758 6367 .. | 6404 6521 6029 6650 | v 6025 6646 1 -138
[24] 6213 1 6758 6367 .. | 6404 6521 6029 6650 | v 6025 6646 1 -138
[25] 6213 1 6758 6367 .. | 6404 6521 6029 6650 | v 6025 6646 1 -138
```

A “stop list” can be used to eliminate false positives.

Ignore “6404 6521 6029 6650” and repeat the experiment:

Total number of image files:	178
Number of CCNs found:	47,737
Number of distinct CCNs:	15,612
Most popular CCN:	5501 8501 3501 3705 (35 times on 27 drives)

Once again, this does not seem to be a valid credit card number:

```
[14] 3201 4901 : |5501 8501 3501 3705| 5102....yes.%d\Off
[112] 3201 4901 : |5501 8501 3501 3705| 5102....yes.%d\Off
[121] 3201 4901 : |5501 8501 3501 3705| 5102....yes.%d\Off
[128] 3201 4901 : |5501 8501 3501 3705| 5102....yes.%d\Off
[133] 3201 4901 : |5501 8501 3501 3705| 5102....yes.%d\Off
[181] 3201 4901 : |5501 8501 3501 3705| 5102....yes.%d\Off
[182] 3201 4901 : |5501 8501 3501 3705| 5102 13505....yes.
[184] 3201 4901 : |5501 8501 3501 3705| 5102 13505....yes.
[186] 3201 4901 : |5501 8501 3501 3705| 5102 13505....yes.
```

Problems with the “stop list” approach:

List must be:

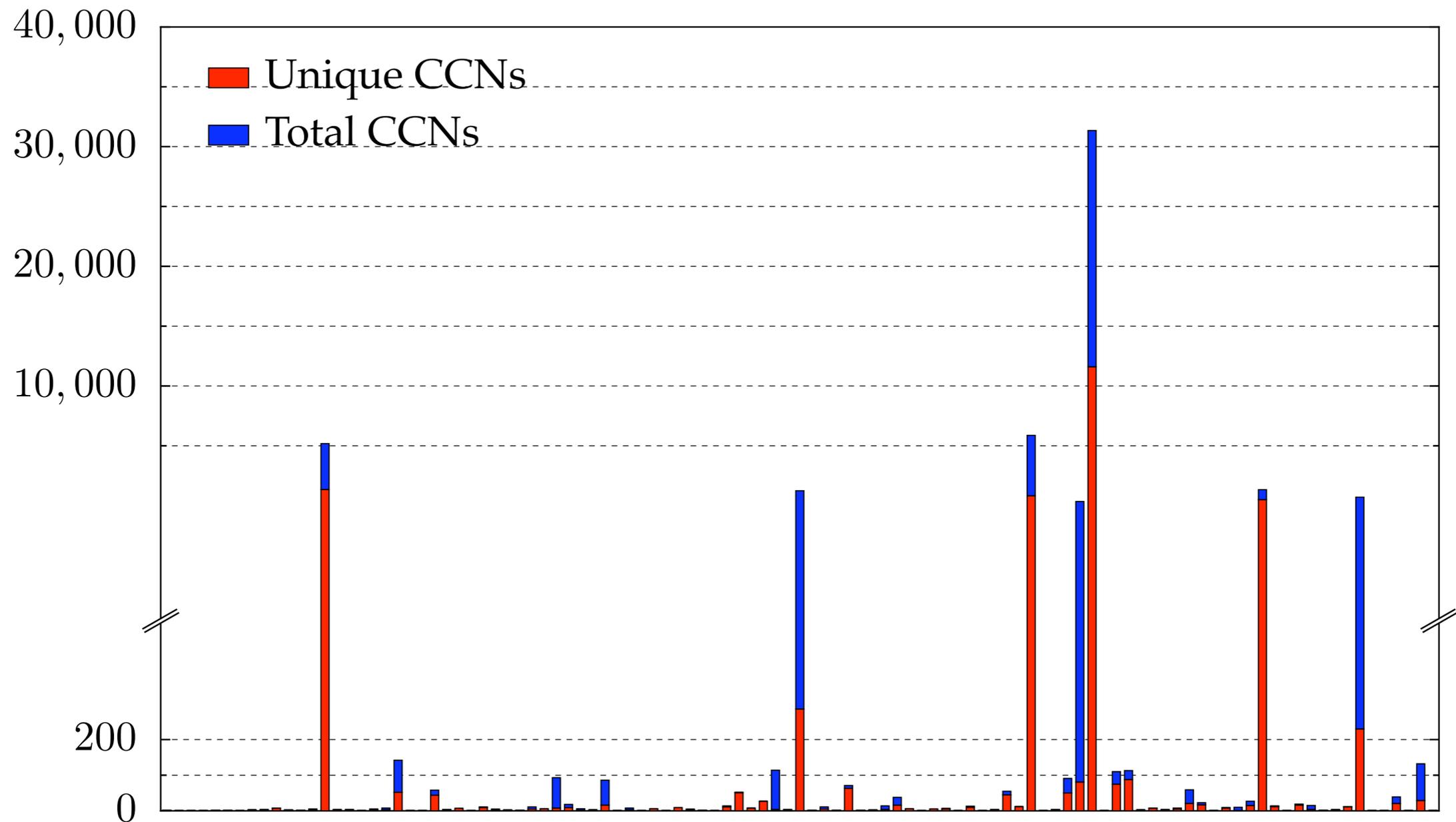
- Constructed
- Maintained
- Tuned for different applications

Building the “stop list” requires:

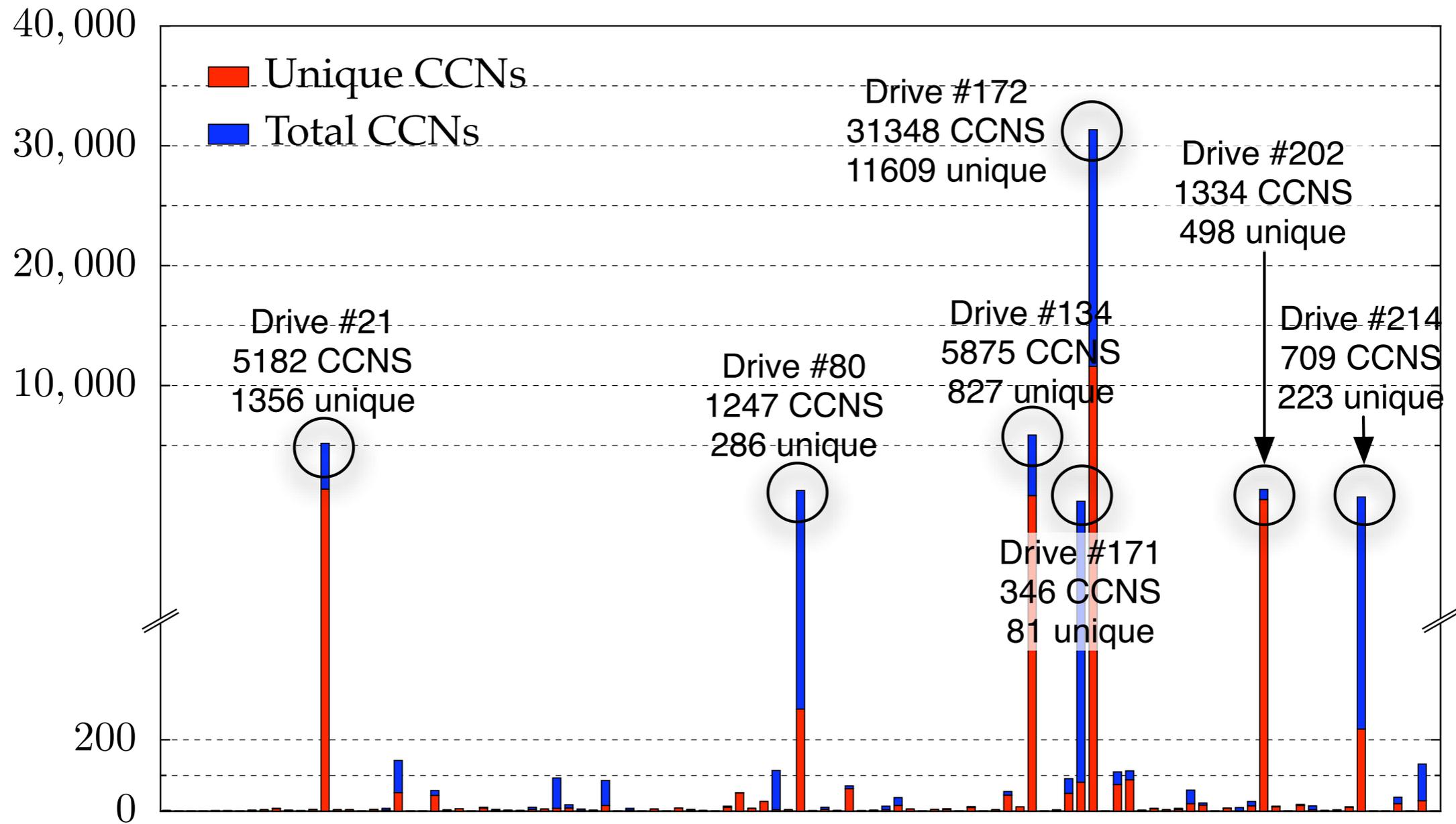
- Judgement
- A large corpus
- Constant Vigilance — items may be included inappropriately.

The stop list throws away information.

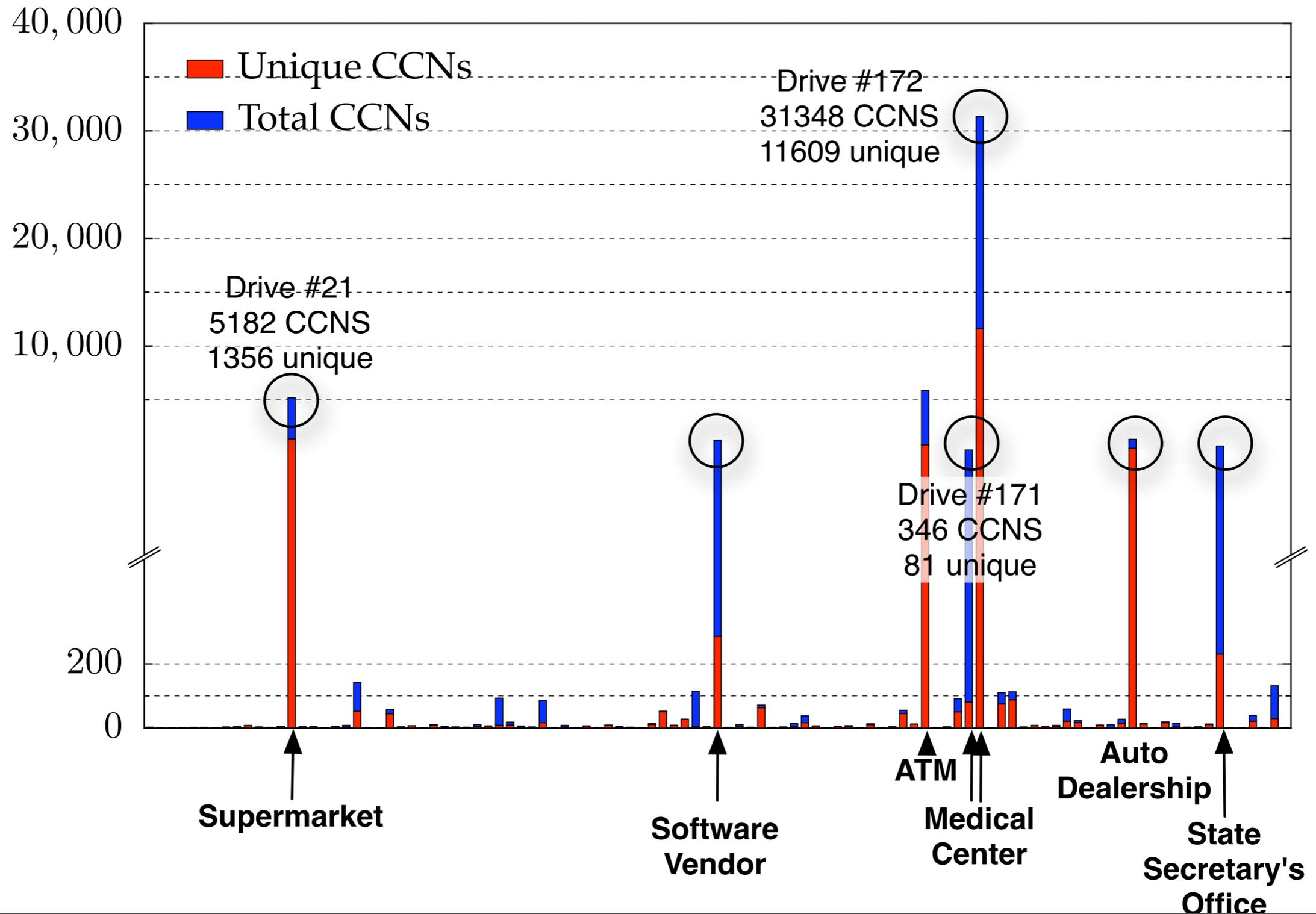
We assume that false positives are rare and focus on drives with high response.



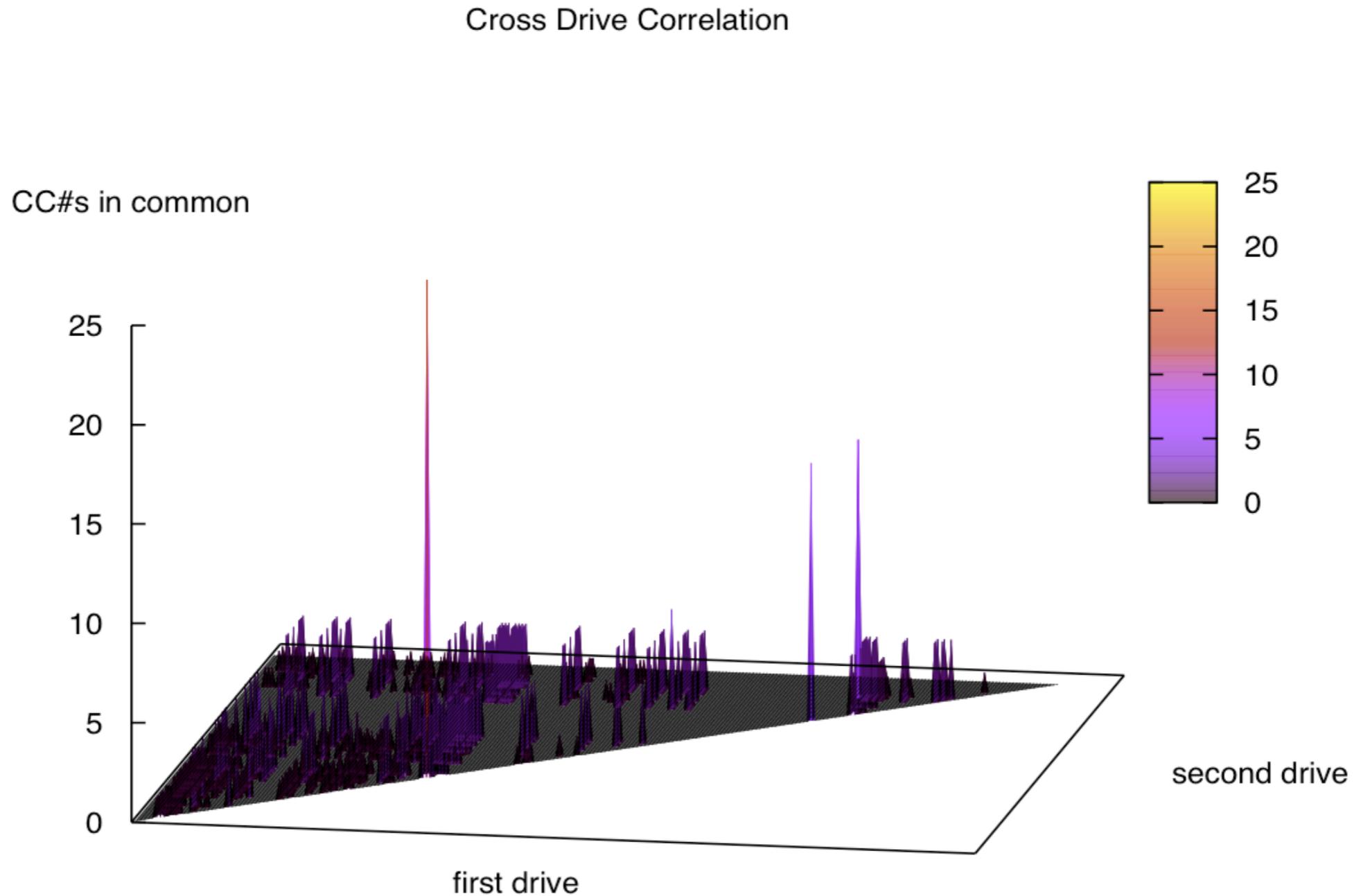
Six drives had more than 400 credit card numbers:



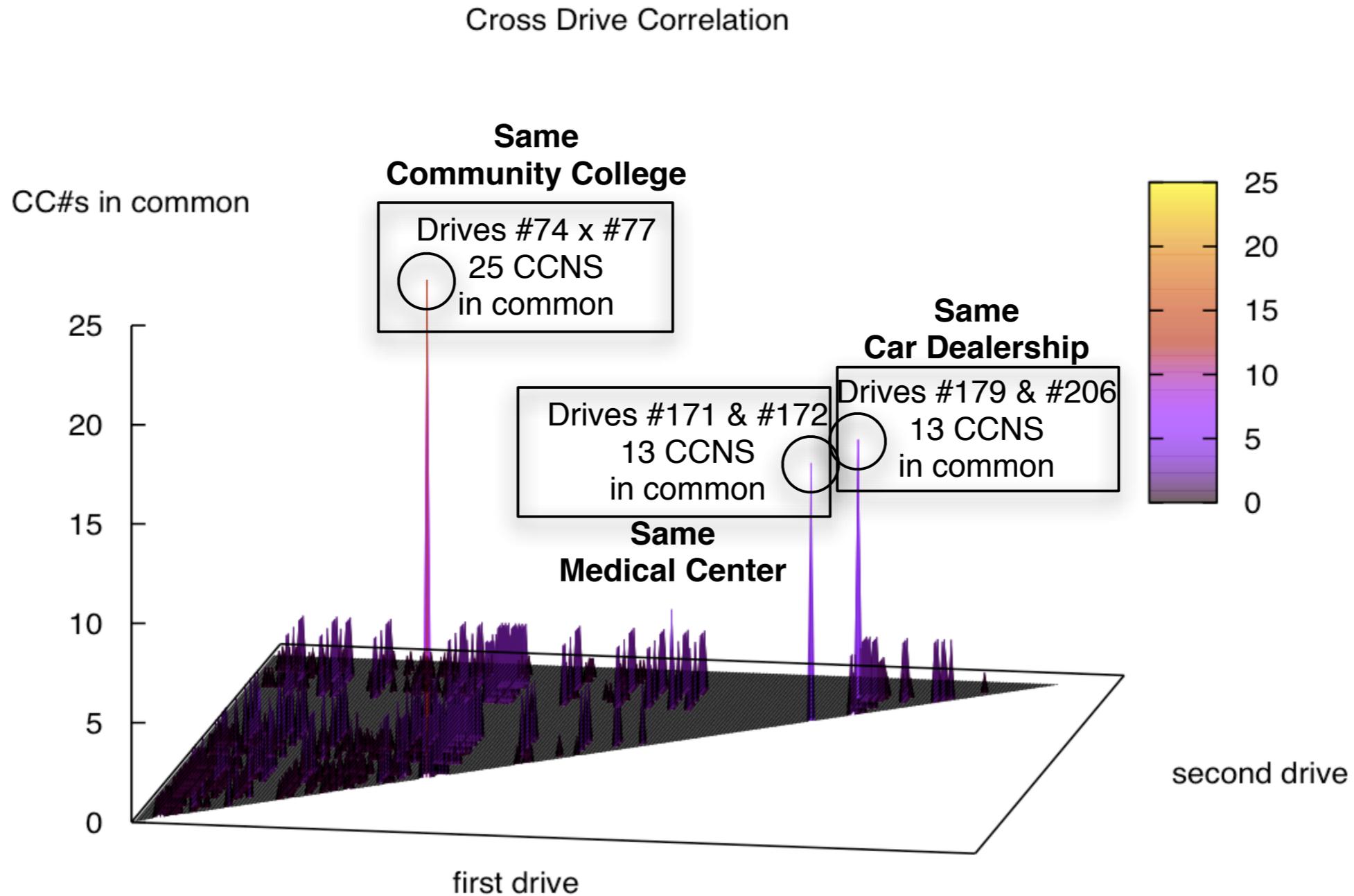
Six drives had more than 400 credit card numbers:



Second-order cross drive analysis correlates pseudo-unique information between drives.



Second-order cross drive analysis correlates pseudo-unique information between drives.

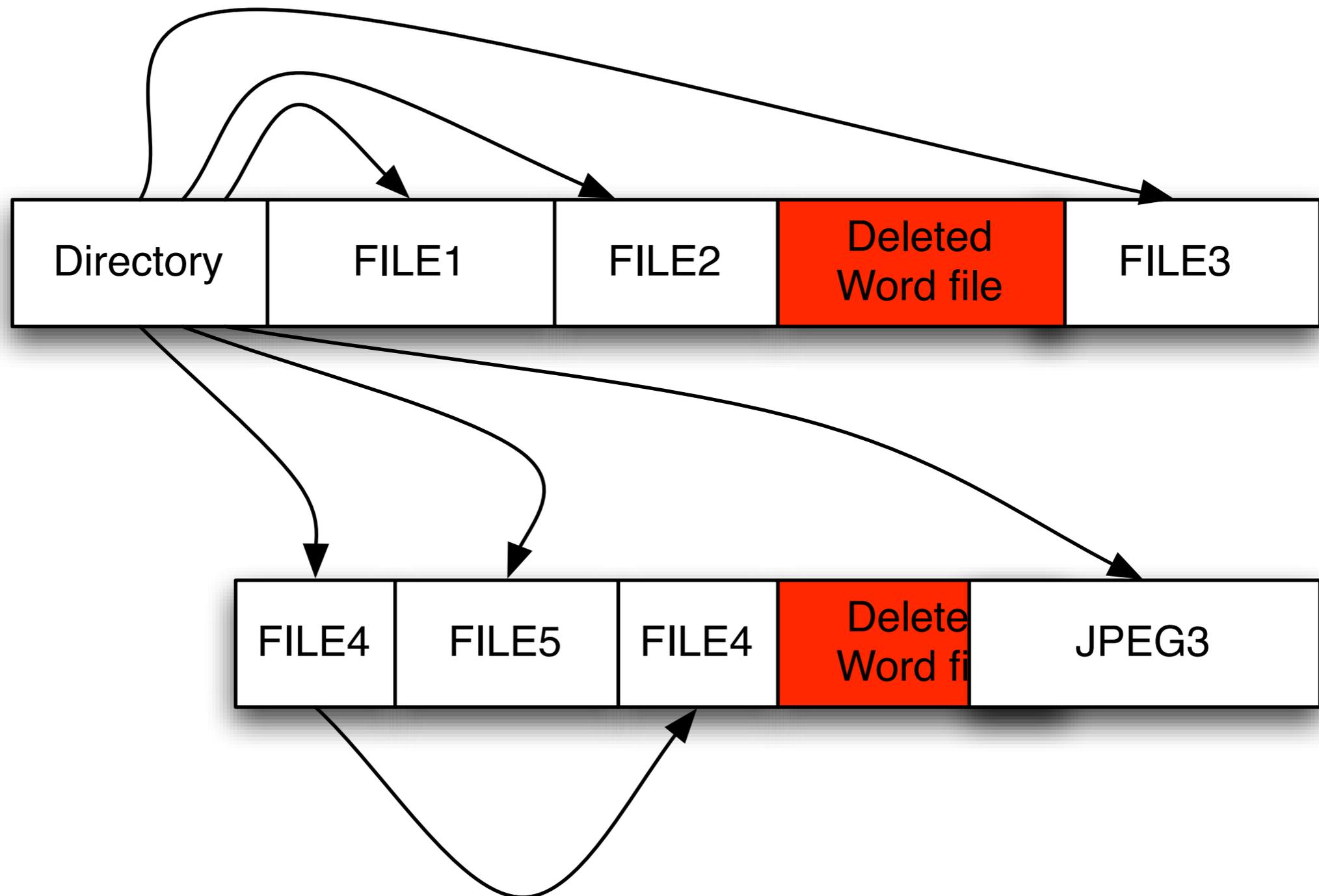




http://www.nps.gov/history/museum/exhibits/band/slideshow/CCC/carving_6.html

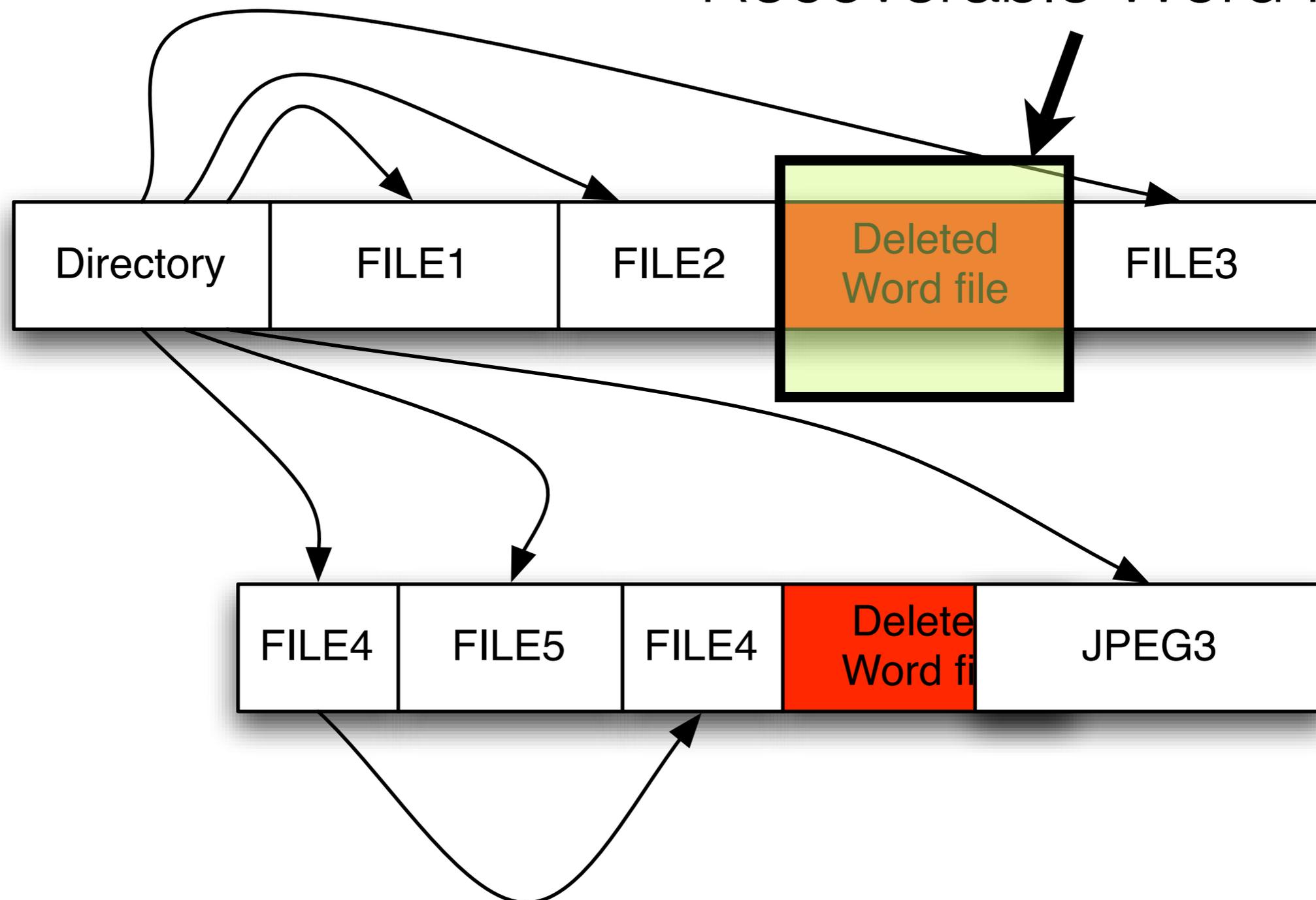
File Carving

“Carving” is the search for objects based on *content*, rather than on metadata.

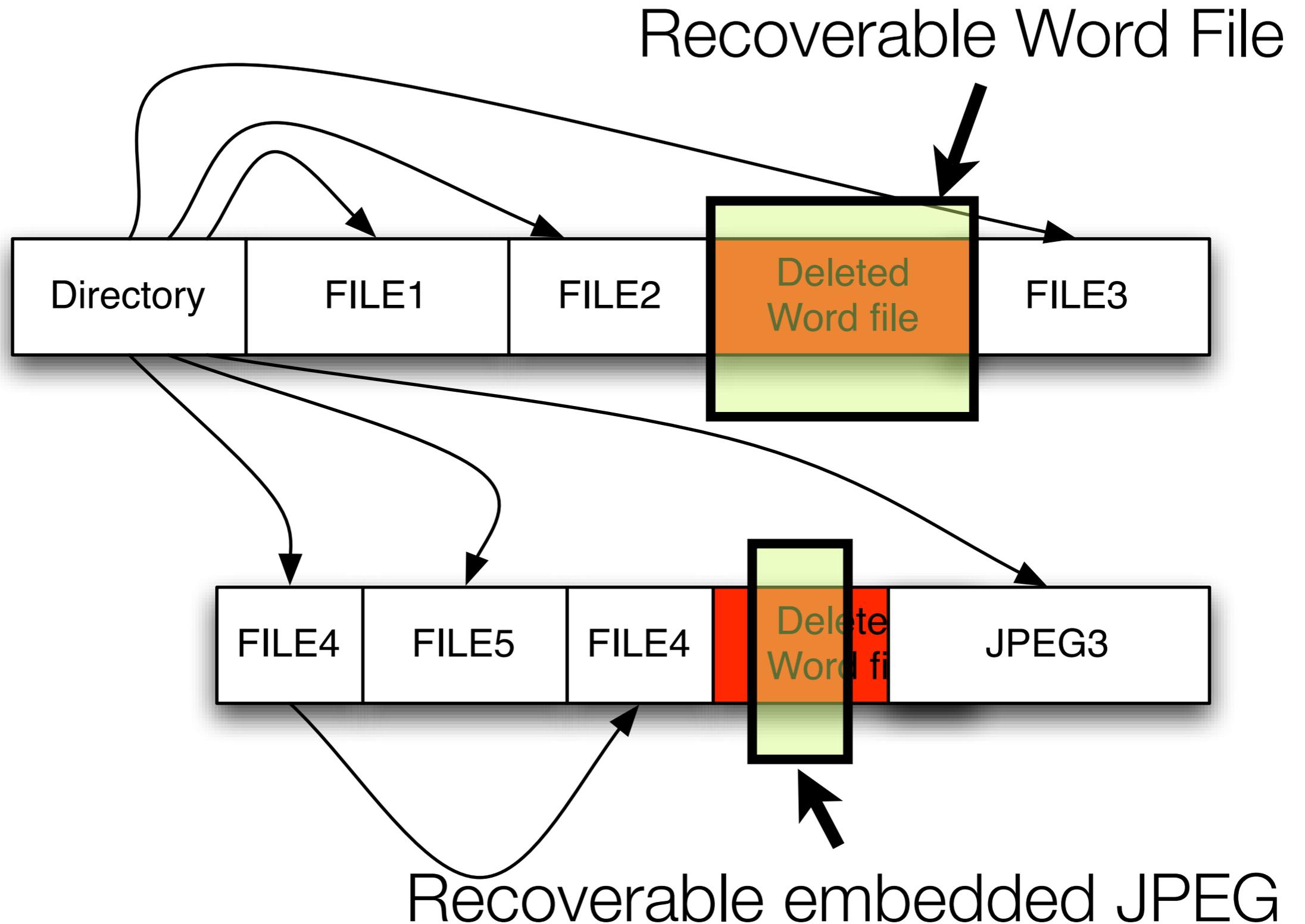


“Carving” is the search for objects based on *content*, rather than on metadata.

Recoverable Word File



“Carving” is the search for objects based on *content*, rather than on metadata.



“Carving” searches for objects based on *content*, rather than on metadata.

What can be carved:

- Disks & Disk Images
- Memory
- Files of unknown format (to find embedded objects)

Objects that can be recovered:

- Images
- Text files & documents
- Cryptographic Keys

Why carve?

- Directory entries are overwritten
- Directory entries are damaged
- File formats aren't known

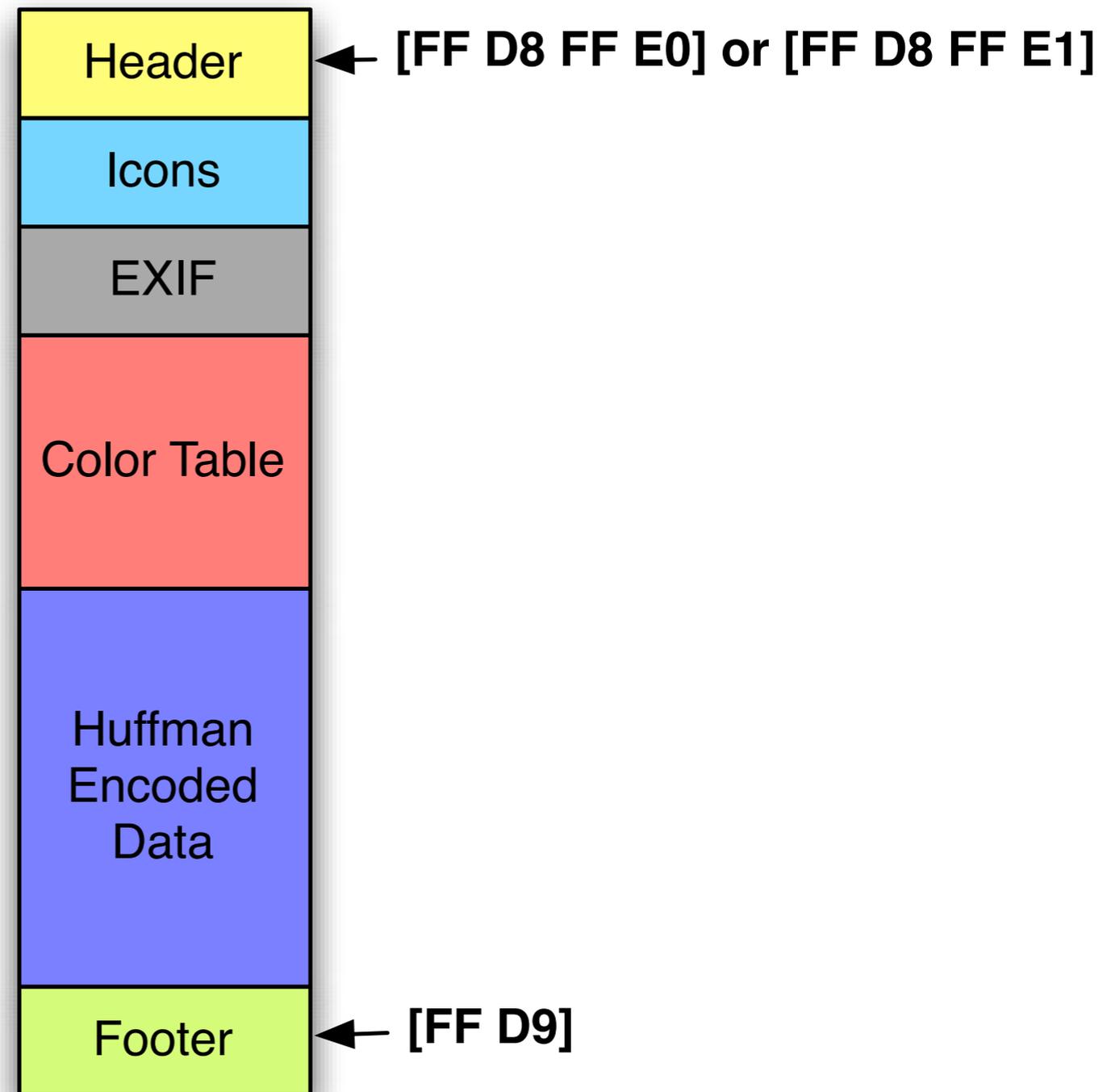
Example: Carving JPEG Files

JPEGs are container files

- Standard Header
- Standard Footer
- Embedded Images

Carving strategy:

- Find all headers
- Find all footers
- Save sectors to files

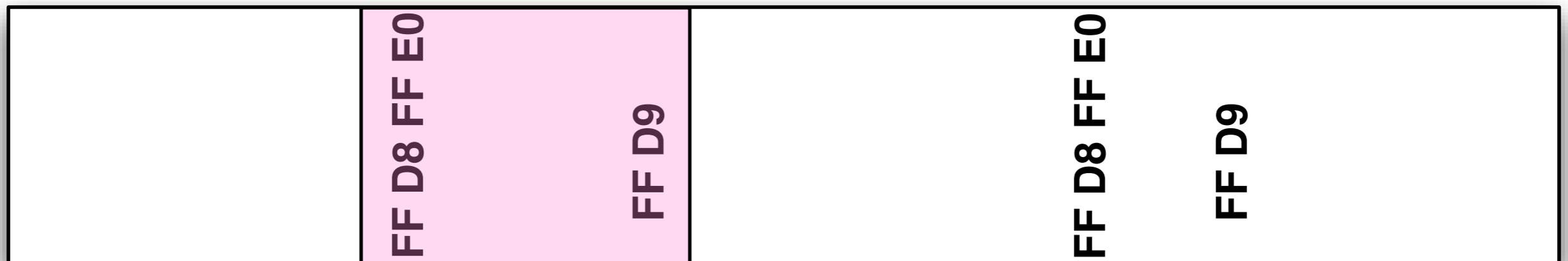


Header/Footer carving with JPEG: Fast, but error prone.



Disk Sectors ➔

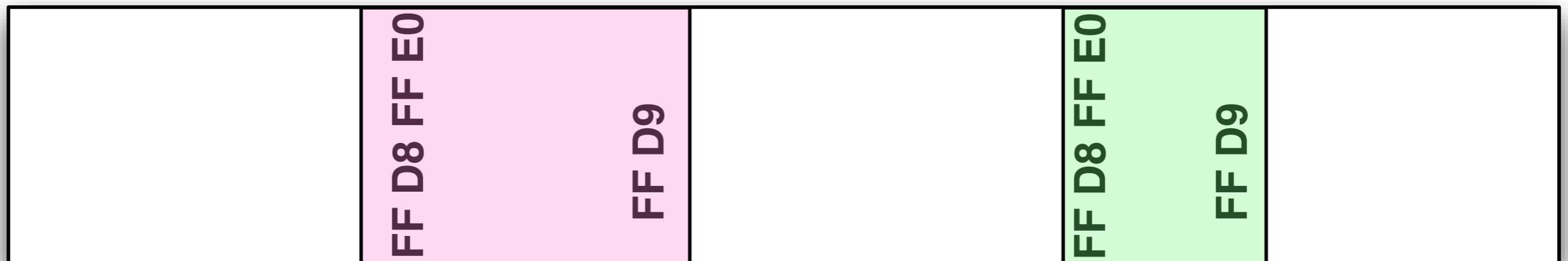
Header/Footer carving with JPEG: Fast, but error prone.



Disk Sectors ➔

Header/Footer carving with JPEG:

Fast, but error prone.



Disk Sectors ➔

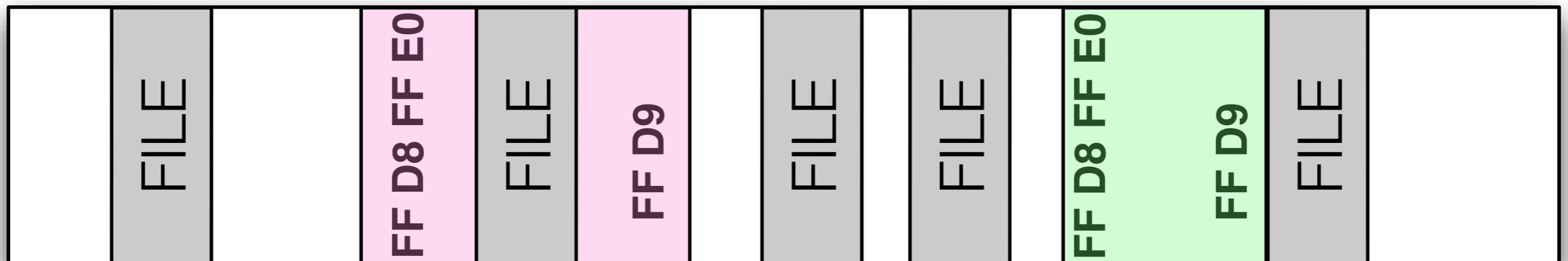
Header/Footer carving with JPEG: Fast, but error prone.



Disk Sectors ➔

This is the strategy used by **foremost** and **scalpel**

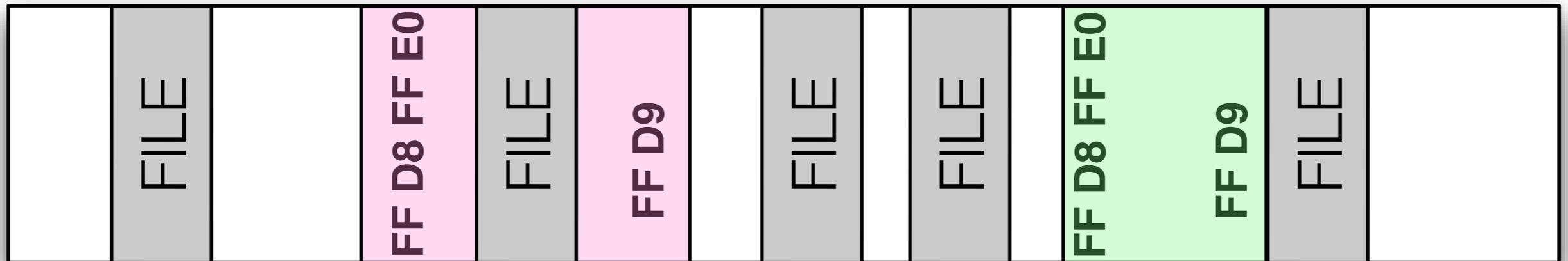
Header/Footer carving with JPEG: Fast, but error prone.



Disk Sectors ➔

This is the strategy used by **foremost** and **scalpel**

Header/Footer carving with JPEG: Fast, but error prone.

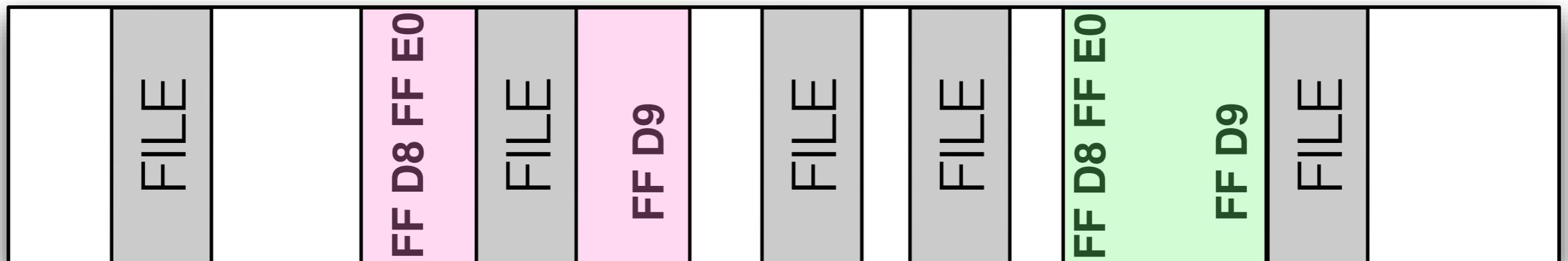


Disk Sectors →

This is the strategy used by **foremost** and **scalpel**



Header/Footer carving with JPEG: Fast, but error prone.

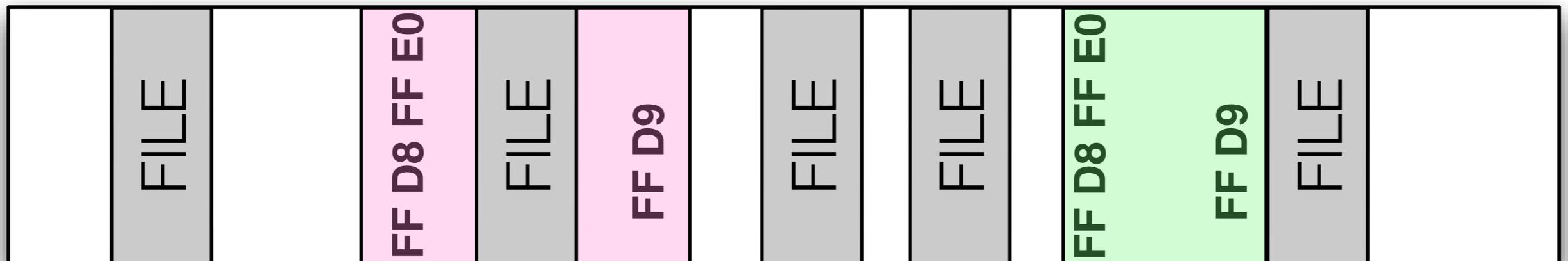


Disk Sectors ➔



This is the strategy used by **foremost** and **scalpel**

Header/Footer carving with JPEG: Fast, but error prone.



Disk Sectors ➔



This is the strategy used by **foremost** and **scalpel**

With simple header/footer carving, objects must be *validated* after they are saved in files (Carving with Validation)

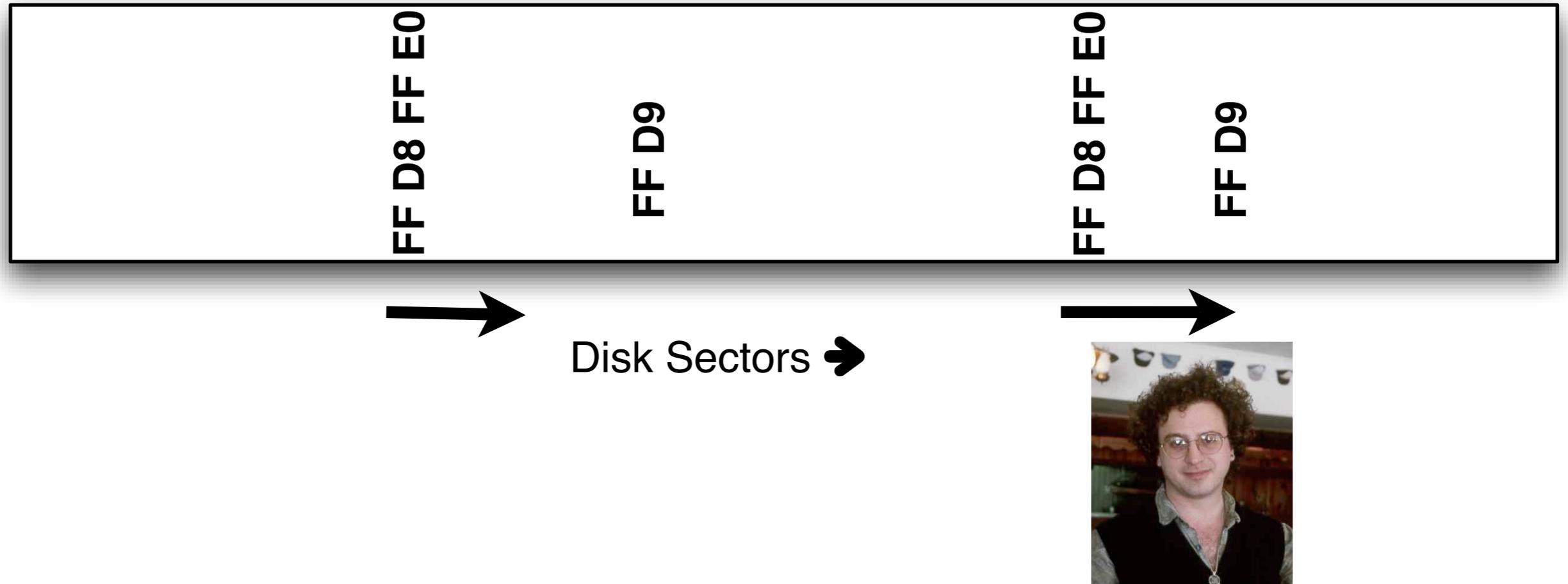
Other simple approaches for carving JPEGs



Header/Maximum size Carving

- Start at header and carve until JPEG file is invalid

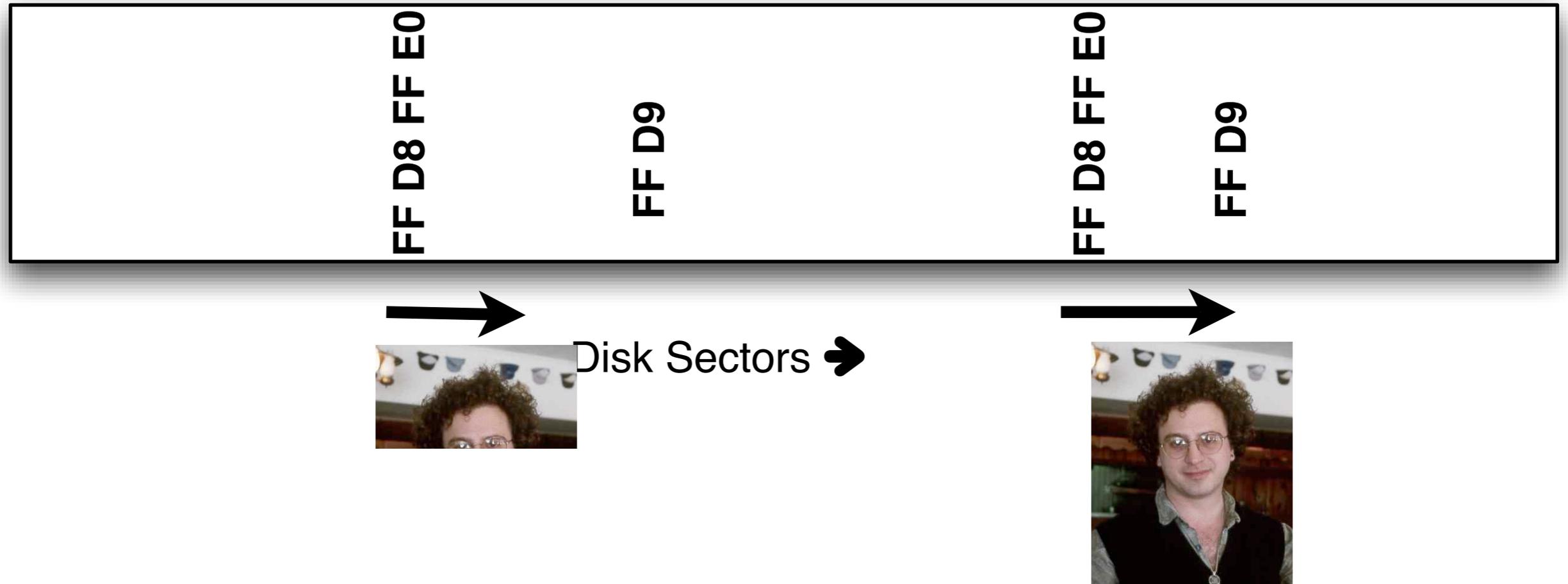
Other simple approaches for carving JPEGs



Header/Maximum size Carving

- Start at header and carve until JPEG file is invalid

Other simple approaches for carving JPEGs



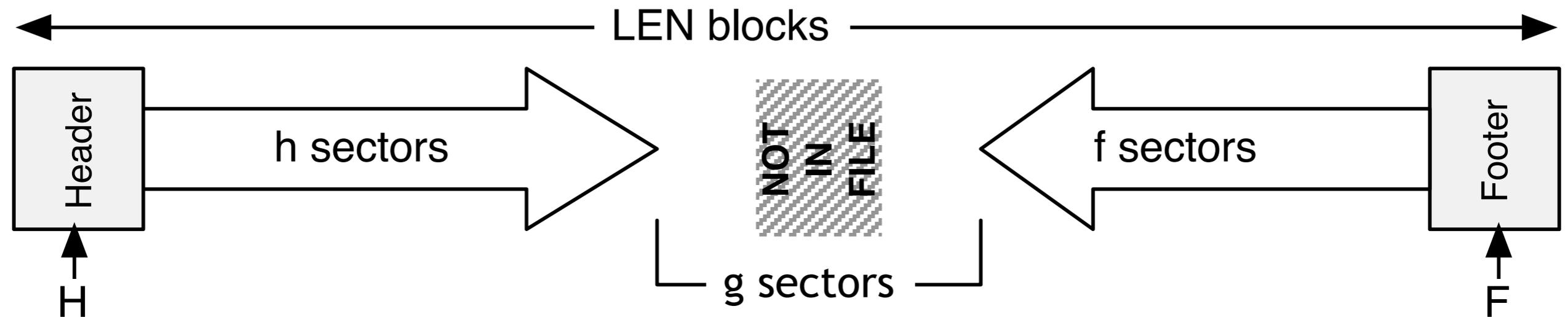
Header/Maximum size Carving

- Start at header and carve until JPEG file is invalid

Fragment Recovery Carving:

Attempts to reassemble fragmented files

Fragment Recovery Carving:



$$LEN = S - F + 1$$

for I in range(0, LEN):

 for J in range(0, LEN - I):

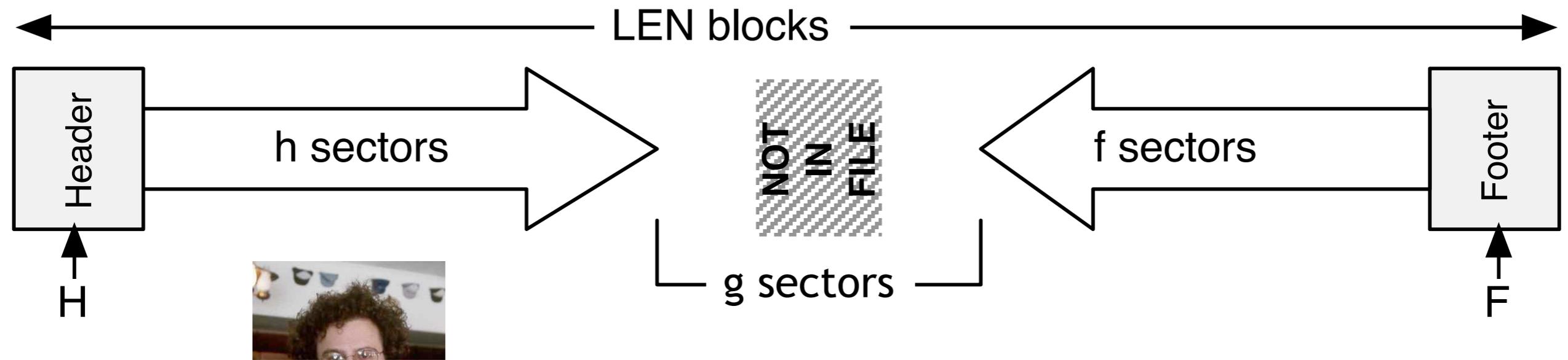
 data = blocks[S:S+I] + blocks[F-J:J]

 if valid(data) == True: save(data)

Fragment Recovery Carving:

Attempts to reassemble fragmented files

Fragment Recovery Carving:



$$LEN = S - F + 1$$

for I in range(0, LEN):

for J in range(0, LEN - I):

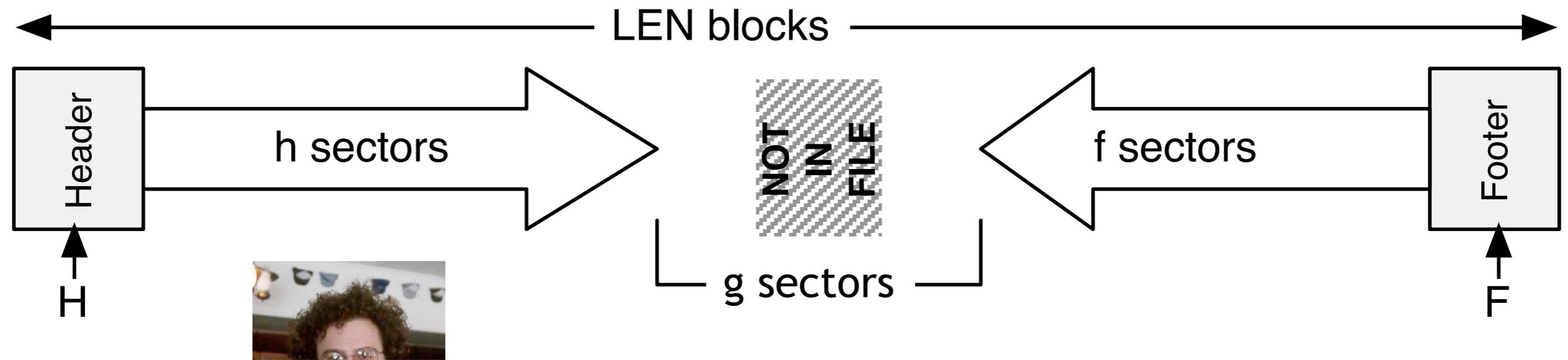
data = blocks[S:S+I] + blocks[F-J:J]

if valid(data) == True: save(data)

Fragment Recovery Carving:

Attempts to reassemble fragmented files

Fragment Recovery Carving:



$$\text{LEN} = S - F + 1$$

for I in range(0, LEN):

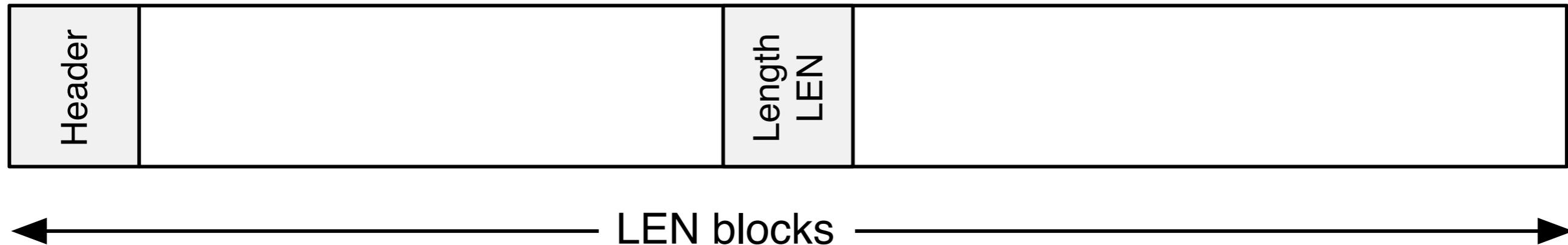
 for J in range(0, LEN - I):

 data = blocks[S:S+I] + blocks[F-J:J]

 if valid(data) == True: save(data)

Header/Length Carving takes advantage of blocks that code a file's length.

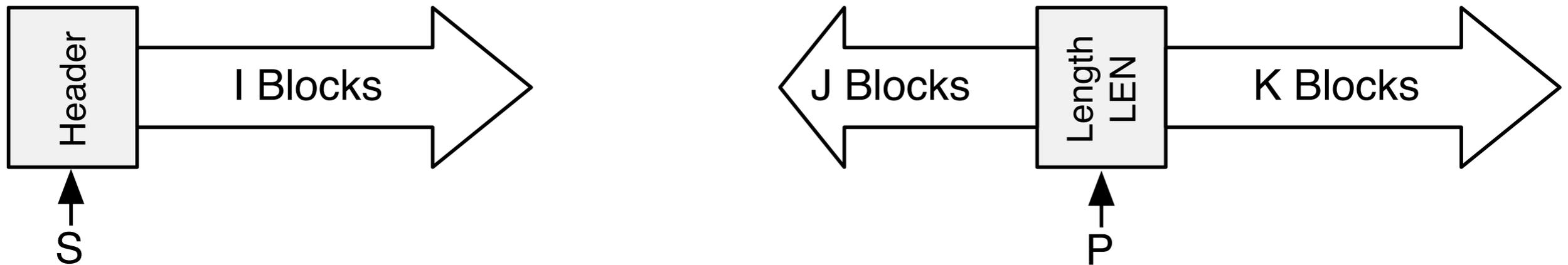
Header/Length sectors: (LEN blocks are found in ZIP & MSOffice)



Header/Embedded Length Carving:

- Looks for structures that code length.
- Works with MS Office and ZIP files

Header/Length Fragment Recovery Carving:



```
for I in range(0,LEN):  
    for J in range(0,LEN-I):  
        K = LEN - (I+J)  
        data = blocks[S:S+I] + blocks[P-J:P+K]  
        if valid(data)==True: save(data)
```

Carving tools available today:

Open Source:

- **Foremost** - Developed by Jesse Kornblum and Kris Kendall at AFOSI
- **Scalpel** - Improved version of Foremost, by Golden G. Richard III
- **CarvFS** - Virtual file system for carving
- **PhotoRec** - Recovers lost photos from hard drives
- **RevIT & S2** - Experimental carvers developed for DFRWS 2006 carving challenge

Commercial:

- **EnCase** - comes with some eScripts that will carve
- **DataLifter** - File Extractor Pro

Scalpel configuration file

```
# To redefine the wildcard character, change the setting below and all
# occurrences in the formost.conf file.
#
#wildcard ?

#           case   size   header           footer
#extension sensitive
#
# GIF and JPG files (very common)
#   gif     y      5000000   \x47\x49\x46\x38\x37\x61   \x00\x3b
#   gif     y      5000000   \x47\x49\x46\x38\x39\x61   \x00\x3b
#   jpg     y      200000000  \xff\xd8\xff\xe0\x00\x10   \xff\xd9
#
#
# PNG
#   png     y      200000000  \x50\x4e\x47?   \xff\xfc\xfd\xfe
#
#
# BMP (used by MSWindows, use only if you have reason to think there are
# BMP files worth digging for. This often kicks back a lot of false
# positives
#
#   bmp     y      100000   BM??\x00\x00\x00
#
# TIFF
#   tif     y      200000000  \x49\x49\x2a\x00
# TIFF
#   tif     y      200000000  \x4D\x4D\x00\x2A
#
```

Uncomment the file types that you want to carve.



Using The Sleuth Kit

Hard drives are divided into partitions

Master Boot Record

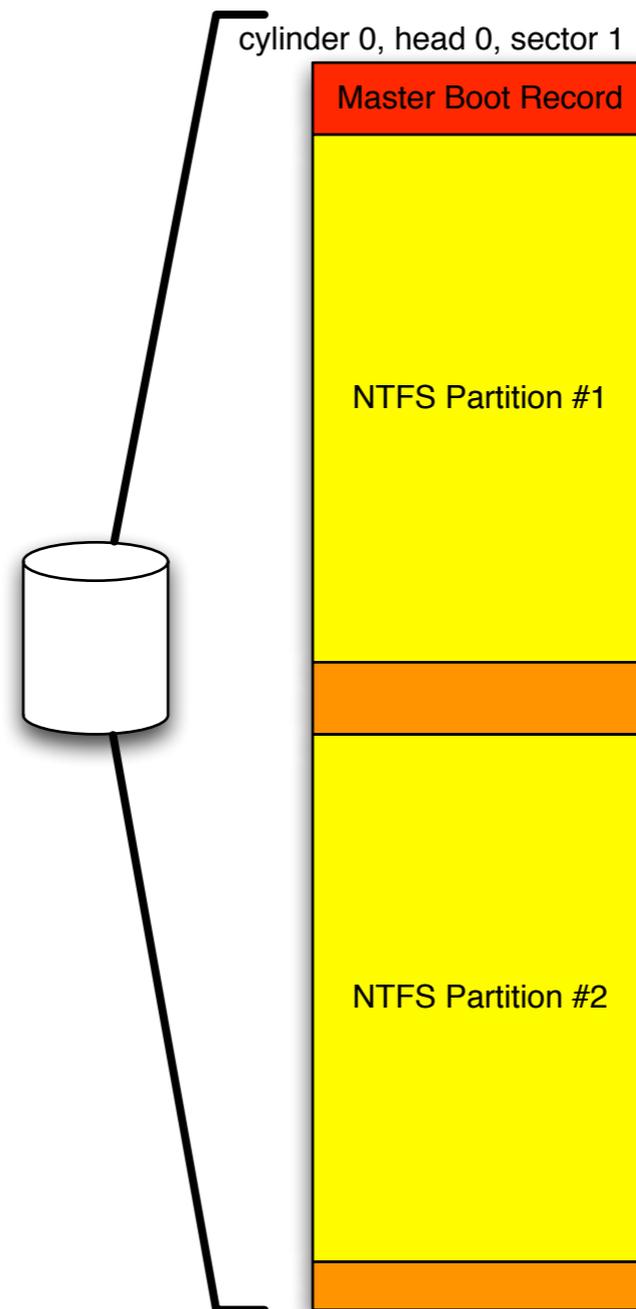
- Designates disk type
- Defines up to 4 partitions
- Specifies bootable partitions
- Partitions sometimes called “slices”

Each Partition:

- May be FAT, NTFS
- May contain internal structure

Note:

- Partitions may be on raw device, without MBR

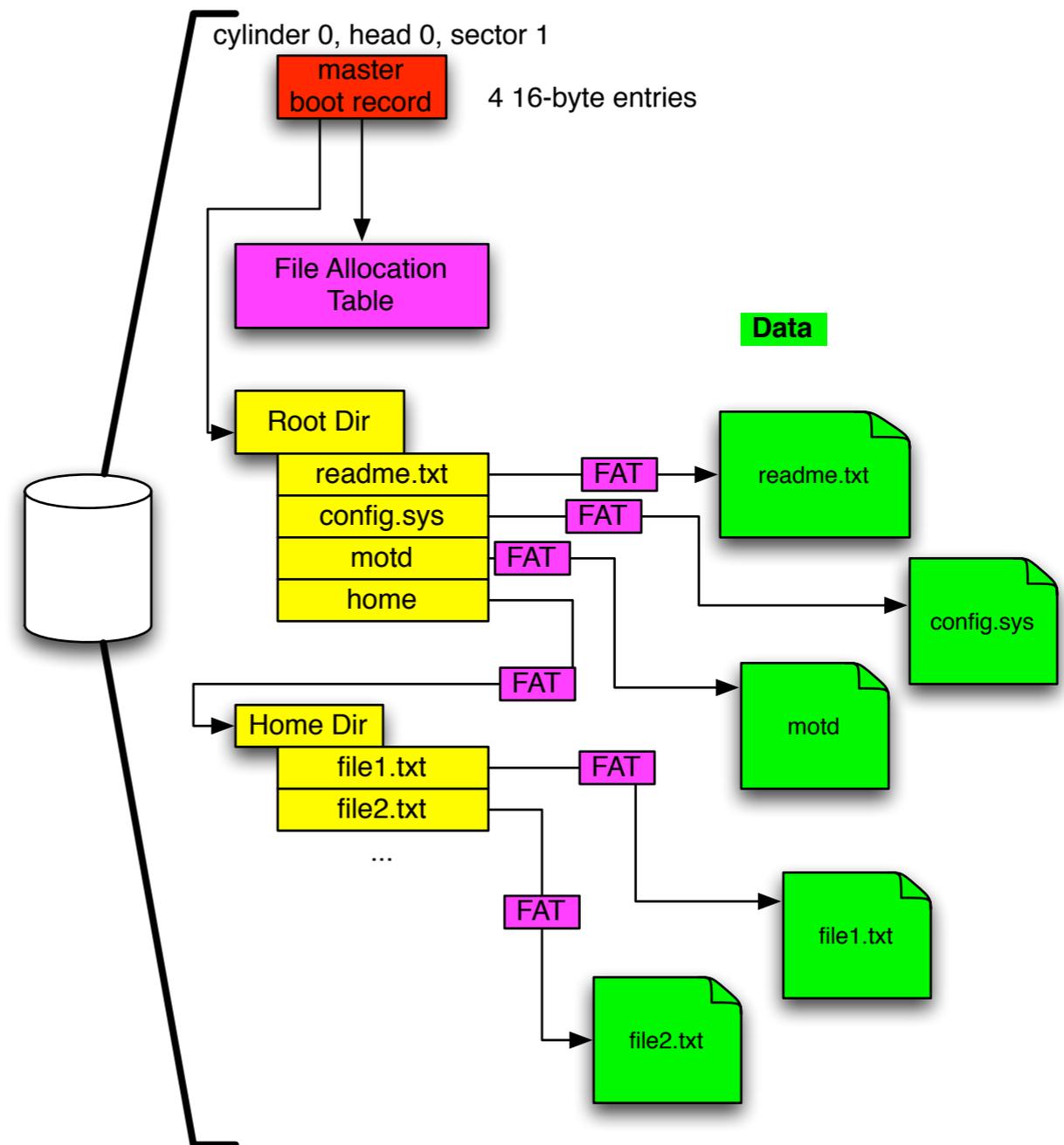


Each partition contains metadata and data

Metadata tells how to work with the disk and the data.

- Partition table
- List of available sectors
- Directory information

Data is the content of files.



The Sleuth Kit (TSK) is a powerful tool for working with disk images.

Command-line tools for working with file systems.

Open source computer forensics toolkit

Originally “The Coroner's Toolkit,” developed by Dan Farmer & Wietse Venema

Rewritten and maintained by Brian Carrier:

- Carrier created a modular internal design. Added image layer, disk tools, FAT recover, 64-bit support, live analysis, UFS2 & EXT3 Journal support....

Today TSK supports:

- Image file formats: raw, AFF, AFD, AFM, EWF, split-raw
- Partitioning schemes: DOS, GPT, Apple, BSD & Solaris
- File Systems: FAT12/16/32, NTFS, ext2/3, UFS1/2, ISO9660, raw, swap
(note: some support is better than others)

Runs on Linux, OSX, Windows, *BSD, Cygwin, Solaris

Autopsy Forensic Browser

Web-based front-end GUI

Four Modes:

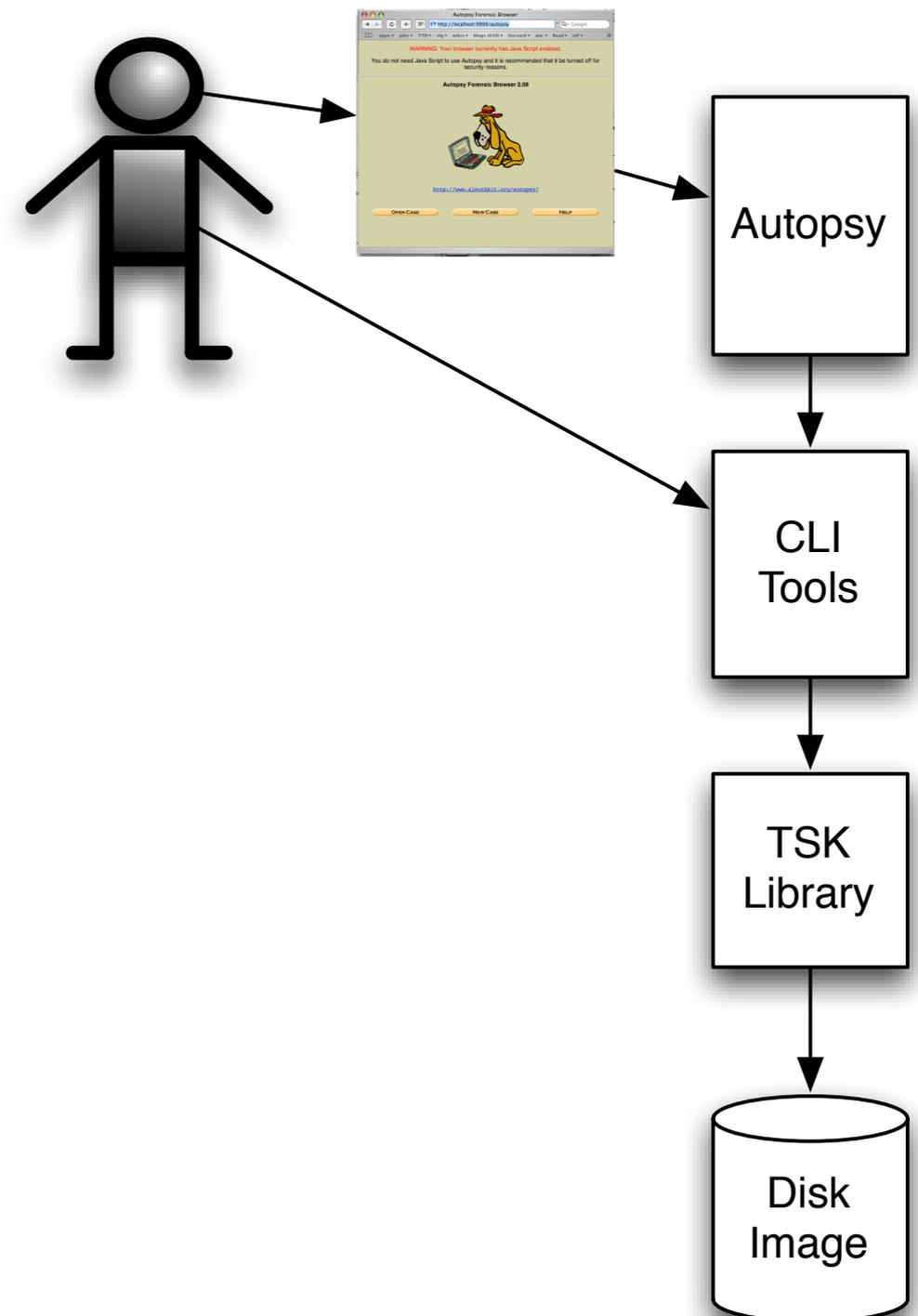
- File Browsing
- Inode Browsing
- Block Browsing
- Keyword Search

Autopsy makes TSK click-able!



TSK is designed as a modular system

You can even write your own programs that call the library directly.



TSK command-line programs divided up by layer.

j-	journal layer
f-	file name layer
i-	metadata (inode) layer
d-	content (data) layer
mm-	volumes/partitions
img_-	Disk images

TSK command-line programs divided by function.

-stat	print status
-ls	list something
-find	find something
-cat	output contents
-calc	compute something

Working with disk images: “img_” and “m” layers

img_cat - copies image to stdout

img_stat - Status about an image

```
$ img_stat /project/p3/1141.aff
IMAGE FILE INFORMATION
-----
Image Type: AFF

Size in bytes: 10239860736

MD5: f87896b1cf361ac1da3780211f423
SHA1: e528af8187781ec379ea5a7f85580be97b92942
Creator: aimage
Image GUID: C336A958753C1733F498F57395E3555
Acquisition Date: 2006-09-19 17:50:43
Acquisition Device: /dev/ad4
AFFLib Version: 1.6.31
Device Model: Maxtor 91024U3
Device SN: H3H15SCC
```

mm_stat - Print which partitioning scheme is in use

mmls - print the partitions

```
$ mmls /project/p3/1141.aff
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors
```

	Slot	Start	End	Length	Description
00:	-----	0000000000	0000000000	0000000001	Primary Table (#0)
01:	-----	0000000001	0000000062	0000000062	Unallocated
02:	00:00	0000000063	0019984859	0019984797	Win95 FAT32 (0x0C)
03:	-----	0019984860	0019999727	0000014868	Unallocated

Tools that work with file systems need to be told the partition offset

`fsstat [-tvV] [-f fstype] [-i imgtype] [-o imgoffset] image - print fs stats`

```
$ fsstat -o 63 /project/p3/1141.aff
FILE SYSTEM INFORMATION
-----
File System Type: FAT32

OEM Name: MSWIN4.1
Volume ID: 0x7cf0a1b
Volume Label (Boot Sector): DRIVE C
Volume Label (Root Directory):
File System Type Label: FAT32
Next Free Sector (FS Info): 930280
Free Sector Count (FS Info): 11867296

Sectors before file system: 63

File System Layout (in sectors)
Total Range: 0 - 19984796
* Reserved: 0 - 31
** Boot Sector: 0
** FS Info Sector: 1
** Backup Boot Sector: 6
* FAT 0: 32 - 9787
* FAT 1: 9788 - 19543
* Data Area: 19544 - 19984796
** Cluster Area: 19544 - 19984791
*** Root Directory: 19544 - 19559
** Non-clustered: 19984792 - 19984796
METADATA INFORMATION
-----
Range: 2 - 319443970
Root Directory: 2

CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 8192
Total Cluster Range: 2 - 1247829

FAT CONTENTS (in sectors)
-----
19544-19559 (16) -> EOF
19560-19575 (16) -> EOF
```

TSK content and metadata tools

Content Category Tools (d)

- dcat - Display contents of a block
- dls - List contents of a block
- dcalc - Maps between dd images and dls results
- dstat - List details about a block

Metadata Category Tools (i)

- ils - list inode details
- istat - displays information about an inode
- icat - displays file contents
- ifind - determine which inode has allocated a block

What's in the root directory?

```
$ fls -o 63 /project/p3/1145.aff
```

```
$ fls -o 63 /project/p3/1141.aff
r/r 3: IO.SYS
r/r * 4:      _UHDLOG.DAT
r/r 5: FRUNLOG.TXT
r/r * 6:      _OMMAND.COM
r/r 7: AUTOEXEC.DOS
d/d 8: WINDOWS
r/r 9: CONFIG.DOS
r/r * 10:     _SDOS.---
d/d 11: DELL
r/r * 12:     _ETUPLOG.TXT
r/r * 13:     _ETLOG.OLD
d/d 14: DMI
d/d * 15:     _ECYCLED
d/d 16: YAMAHA
r/r * 17:     _ETLOG.TXT
r/r 18: ZZ.EXE
r/r * 19:     _YSTEM.1ST
r/r * 20:     _ETLOG.TXT
r/r 21: SETUPXLG.TXT
r/r 22: VIDEOROM.BIN
r/r 23: ZZTOP.BAT
r/r 24: OEMROM.BIN
d/d 25: CDROM
d/d 26: BACKUP
r/r 27: DELL.SDR
r/r 28: CHOICE.COM
d/d 29: ATI
d/d 31: DellUtil
r/r 32: Z2.BAT
d/d 34: Program Files
d/d * 36:     My Documents
r/r * 38:     msdos.sys
r/r * 39:     _UTOEXEC.BAT
r/r * 40:     _ONFIG.SYS
r/r 41: DRIVE C      (Volume Label Entry)
```

What's in the WINDOWS directory?

```
fls -o 63 -m 'WINDOWS' /project/p3/1141.aff
```

```
0|Windows/IO.SYS|0|3|32841|-/---x--x--x|1|0|0|0|110080|1036990800|960498000|997287596|512|0
0|Windows/_UHDLOG.DAT (deleted)|0|4|33279|-/rwxrwxrwx|0|0|0|0|5166|1005627600|997287598|997286916|512|0
0|Windows/FRUNLOG.TXT|0|5|33279|-/rwxrwxrwx|1|0|0|0|2665|1021953600|941040768|941040766|512|0
0|Windows/_OMMAND.COM (deleted)|0|6|33279|-/rwxrwxrwx|0|0|0|0|93040|1036990800|960498000|997287596|512|0
0|Windows/AUTOEXEC.DOS|0|7|33133|-/r-xr-xr-x|1|0|0|0|205|1005627600|996863598|0|512|0
0|Windows/WINDOWS|0|8|16895|d/drwxrwxrwx|1|0|0|0|24576|1037682000|941039802|0|512|0
0|Windows/CONFIG.DOS|0|9|33133|-/r-xr-xr-x|1|0|0|0|262|1001476800|997206694|997206692|512|0
0|Windows/_SDOS.--- (deleted)|0|10|33279|-/rwxrwxrwx|0|0|0|0|1646|1001476800|926693360|0|512|0
0|Windows/DELL|0|11|16895|d/drwxrwxrwx|1|0|0|0|8192|940996800|941039802|0|512|0
0|Windows/_ETUPLUG.TXT (deleted)|0|12|33279|-/rwxrwxrwx|0|0|0|0|235021|1036990800|1002545186|997285806|512|0
0|Windows/_ETLOG.OLD (deleted)|0|13|33279|-/rwxrwxrwx|0|0|0|0|74454|1001476800|997206680|997206606|512|0
0|Windows/DMI|0|14|16895|d/drwxrwxrwx|1|0|0|0|8192|947826000|947863326|947863324|512|0
0|Windows/_ECYCLED (deleted)|0|15|16895|d/drwxrwxrwx|0|0|0|0|57344|984978000|984978354|984978352|512|0
0|Windows/YAMAHA|0|16|16895|d/drwxrwxrwx|1|0|0|0|8192|940996800|941040880|941040878|512|0
0|Windows/_ETLOG.TXT (deleted)|0|17|33279|-/rwxrwxrwx|0|0|0|0|26154|1001476800|997288128|0|512|0
0|Windows/ZZ.EXE|0|18|33133|-/r-xr-xr-x|1|0|0|0|122512|1036990800|925441548|0|512|0
0|Windows/_YSTEM.1ST (deleted)|0|19|33279|-/rwxrwxrwx|0|0|0|0|1679392|1001476800|997287596|997287594|512|0
0|Windows/_ETLOG.TXT (deleted)|0|20|33279|-/rwxrwxrwx|0|0|0|0|7445|1001476800|997287762|997287694|512|0
0|Windows/SETUPXLG.TXT|0|21|33279|-/rwxrwxrwx|1|0|0|0|221|1021953600|985157602|985157602|512|0
0|Windows/VIDEOROM.BIN|0|22|33133|-/r-xr-xr-x|1|0|0|0|32768|1001476800|941041124|0|512|0
0|Windows/ZZTOP.BAT|0|23|33133|-/r-xr-xr-x|1|0|0|0|1489|1021953600|925441596|0|512|0
0|Windows/OEMROM.BIN|0|24|33279|-/rwxrwxrwx|1|0|0|0|36864|1021953600|906497134|0|512|0
0|Windows/CDROM|0|25|16895|d/drwxrwxrwx|1|0|0|0|8192|940996800|941040662|0|512|0
0|Windows/BACKUP|0|26|16895|d/drwxrwxrwx|1|0|0|0|8192|940996800|941040698|0|512|0
0|Windows/DELL.SDR|0|27|32841|-/---x--x--x|1|0|0|0|3336|1021953600|941040702|0|512|0
0|Windows/CHOICE.COM|0|28|33133|-/r-xr-xr-x|1|0|0|0|1754|1021953600|925441458|0|512|0
0|Windows/ATI|0|29|16895|d/drwxrwxrwx|1|0|0|0|8192|940996800|941040824|941040822|512|0
0|Windows/DellUtil|0|31|16895|d/drwxrwxrwx|1|0|0|0|8192|940996800|941040878|941040876|512|0
0|Windows/ZZ.BAT|0|32|33133|-/r-xr-xr-x|1|0|0|0|14|1021953600|925441528|0|512|0
0|Windows/Program Files|0|34|16603|d/d-wx-wx-wx|1|0|0|0|8192|1037941200|941039802|0|512|0
0|Windows/My Documents (deleted)|0|36|16895|d/drwxrwxrwx|0|0|0|0|8192|1036990800|941041156|941041154|512|0
0|Windows/msdos.sys (deleted)|0|38|33279|-/rwxrwxrwx|0|0|0|0|1689|1001476800|997287922|0|512|0
0|Windows/_UTOEXEC.BAT (deleted)|0|39|33133|-/r-xr-xr-x|0|0|0|0|258|1036990800|1032279588|997288316|512|0
0|Windows/_ONFIG.SYS (deleted)|0|40|33133|-/r-xr-xr-x|0|0|0|0|0|1036990800|1032279588|1032279468|512|0
0|Windows/DRIVE C (Volume Label Entry)|0|41|33279|-/rwxrwxrwx|1|0|0|0|0|998798400|998870676|998870674|512|0
```

What's the content of inode 7 (AUTOEXEC.DOS?)

r/r 7: AUTOEXEC.DOS

```
$ icat -o 63 /project/p3/1141.aff 7
@ECHO OFF
SET BLASTER=A220 I5 D1 T4
REM [Header]

REM [CD-ROM Drive]
REM C:\WINDOWS\COMMAND\MSCDEX /D:MSCD001

REM [Miscellaneous]

REM [Display]

SET WIN32DMIPATH=C:\DMI\
SET PATH=C:\DMI\BIN
```

TSK includes higher-level tools for performing forensic analysis.

Timeline tools - Display files based on access and change times

Hash database tools - Identify known files using hash databases

File sorting tools - Sort files based on file type

Image format tools - Convert between image formats

Example: Making a timeline with Sleuth Kit

http://www.sleuthkit.org/sleuthkit/docs/ref_timeline.html

1. Gather file data with fls

```
fls -o 63 -f fat32 -m / -r /project/p3/1146.aff >
data.txt
```

2. Gather unallocated metadata with ils

```
ils -o 63 -f fat32 -m /project/p3/1141.aff >> data.txt
```

3. Run Mactimes

```
mactime -z EST5EDT -b data.txt > timeline.txt
```

mactime sample output...

```
Thu Feb 27 2003 01:56:14      8192 m.. -/-r-xr-xr-x 0      0      299702278 /Documents and Settings/
Butch1/Local Settings/Application Data/Microsoft/Windows/UsrClass.dat
      1024 m.. -/-r-xr-xr-x 0      0      299702281 /Documents and Settings/
Butch1/Local Settings/Application Data/Microsoft/Windows/UsrClass.dat.LOG
      1024 m.. -/-r-xr-xr-x 0      0      294108706 /Documents and Settings/
Butch1/ntuser.dat.LOG
      1472 ..c -/-rwxrwxrwx 0      0      111576080 /WINNT/system32/NtmsData/
_TMSJRNL (deleted)
      180 m.. -/-r-xr-xr-x 0      0      294108707 /Documents and Settings/
Butch1/ntuser.ini
      1472 ..c -rwxrwxrwx 0      0      111576080 <1141.aff-_TMSJRNL-
dead-111576080>
      64 m.. -/-rwxrwxrwx 0      0      301024782 /WINNT/CSC/00000001
196608 m.. -/-r-xr-xr-x 0      0      294108677 /Documents and Settings/
Butch1/NTUSER.DAT
Thu Feb 27 2003 01:56:16      352 m.. -/-rwxrwxrwx 0      0      286523598 /WINNT/SchedLgU.Txt
      65536 m.. -/-rwxrwxrwx 0      0      286523958 /WINNT/system32/config/
SysEvent.Evt
      65536 m.. -/-rwxrwxrwx 0      0      286523956 /WINNT/system32/config/
SecEvent.Evt
      6 m.. -/-r-xr-xr-x 0      0      301335047 /WINNT/Tasks/SA.DAT
      65536 m.. -/-rwxrwxrwx 0      0      286523954 /WINNT/system32/config/
AppEvent.Evt
Thu Feb 27 2003 01:56:18  102400 m.. -/-rwxrwxrwx 0      0      111576072 /WINNT/system32/NtmsData/
NTMSDATA.BAK
      102400 m.. -/-rwxrwxrwx 0      0      111576069 /WINNT/system32/NtmsData/
NTMSDATA
      80312 m.. -/-rwxrwxrwx 0      0      111576070 /WINNT/system32/NtmsData/
NTMSIDX
      1472 m.. -/-rwxrwxrwx 0      0      111576080 /WINNT/system32/NtmsData/
_TMSJRNL (deleted)
      1472 m.. -rwxrwxrwx 0      0      111576080 <1141.aff-_TMSJRNL-
dead-111576080>
```

Autopsy: A graphical interface to TSK.

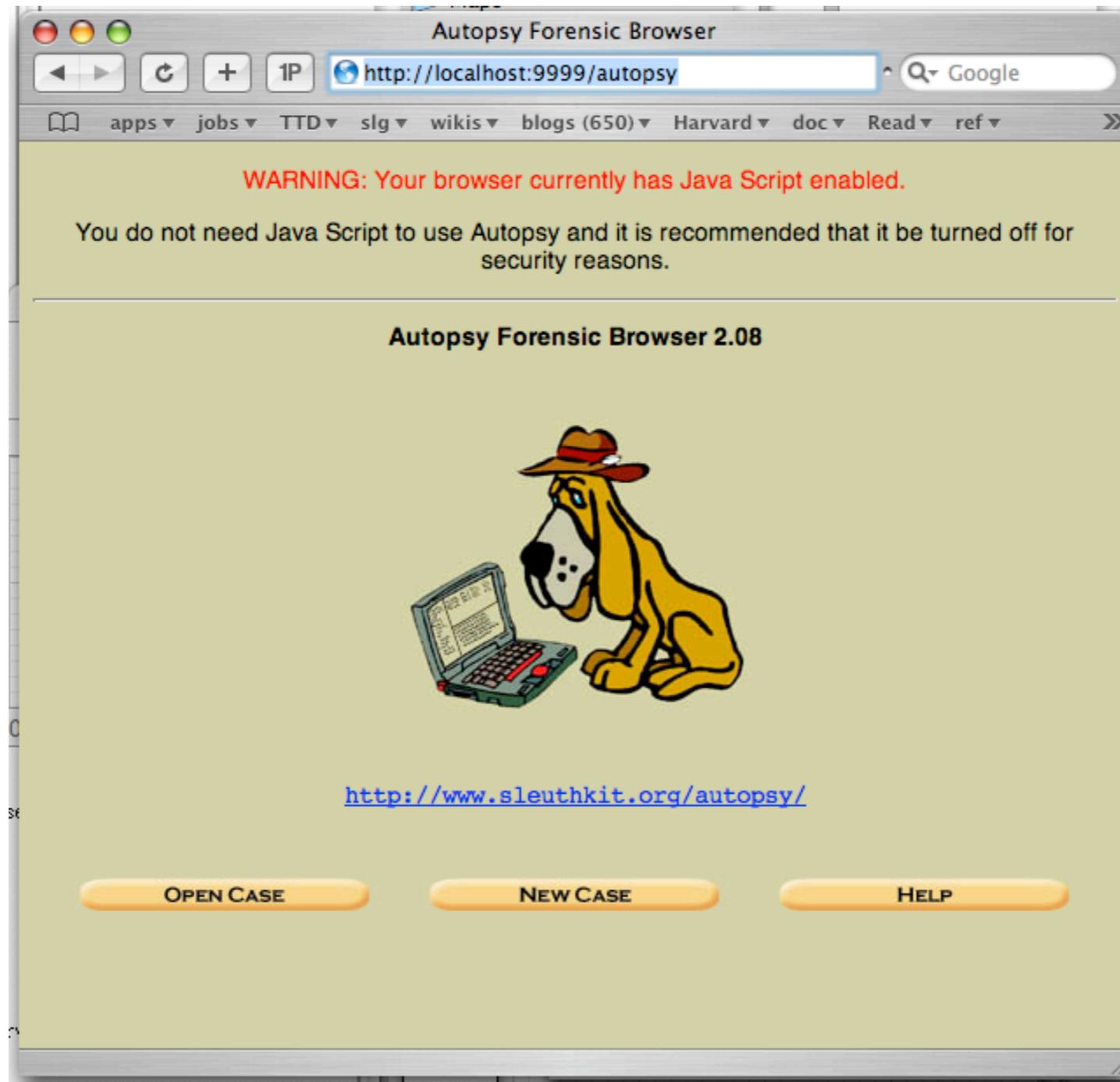
Web-based interface.

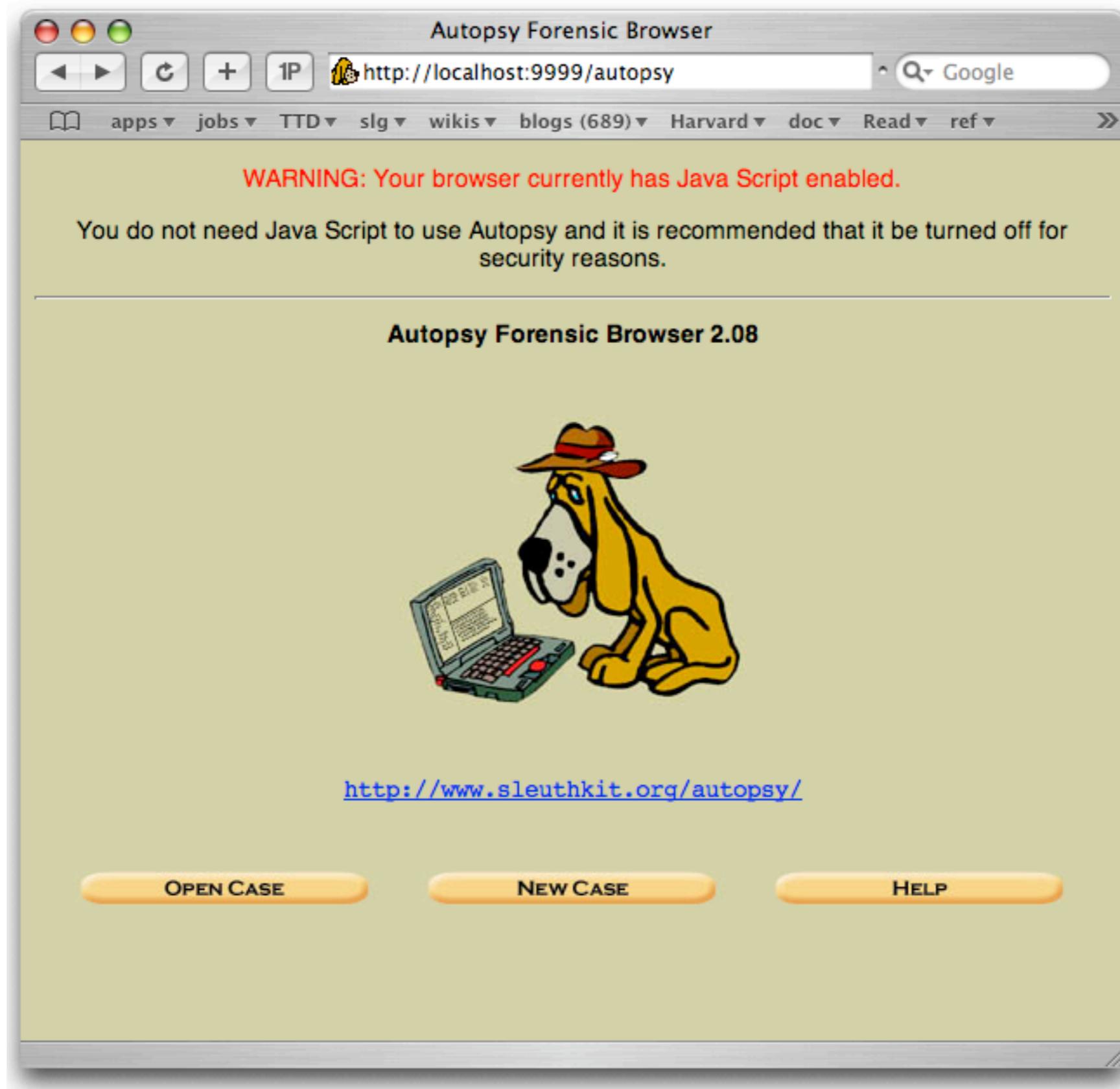
- Autopsy is a perl program
- Listens on port 9999, only from Localhost
- Use SSH tunneling to run on a different machine

“Dumb Interface”

- Most state is kept in the client, not the server
- Runs TSK command-line tools

```
% ssh -L9999:localhost:9999 192.168.1.5
```





Create A New Case

http://localhost:9999/autopsy?mod=0&view=1

apps jobs TTD slg wikis blogs (689) Harvard doc Read ref

CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

1145

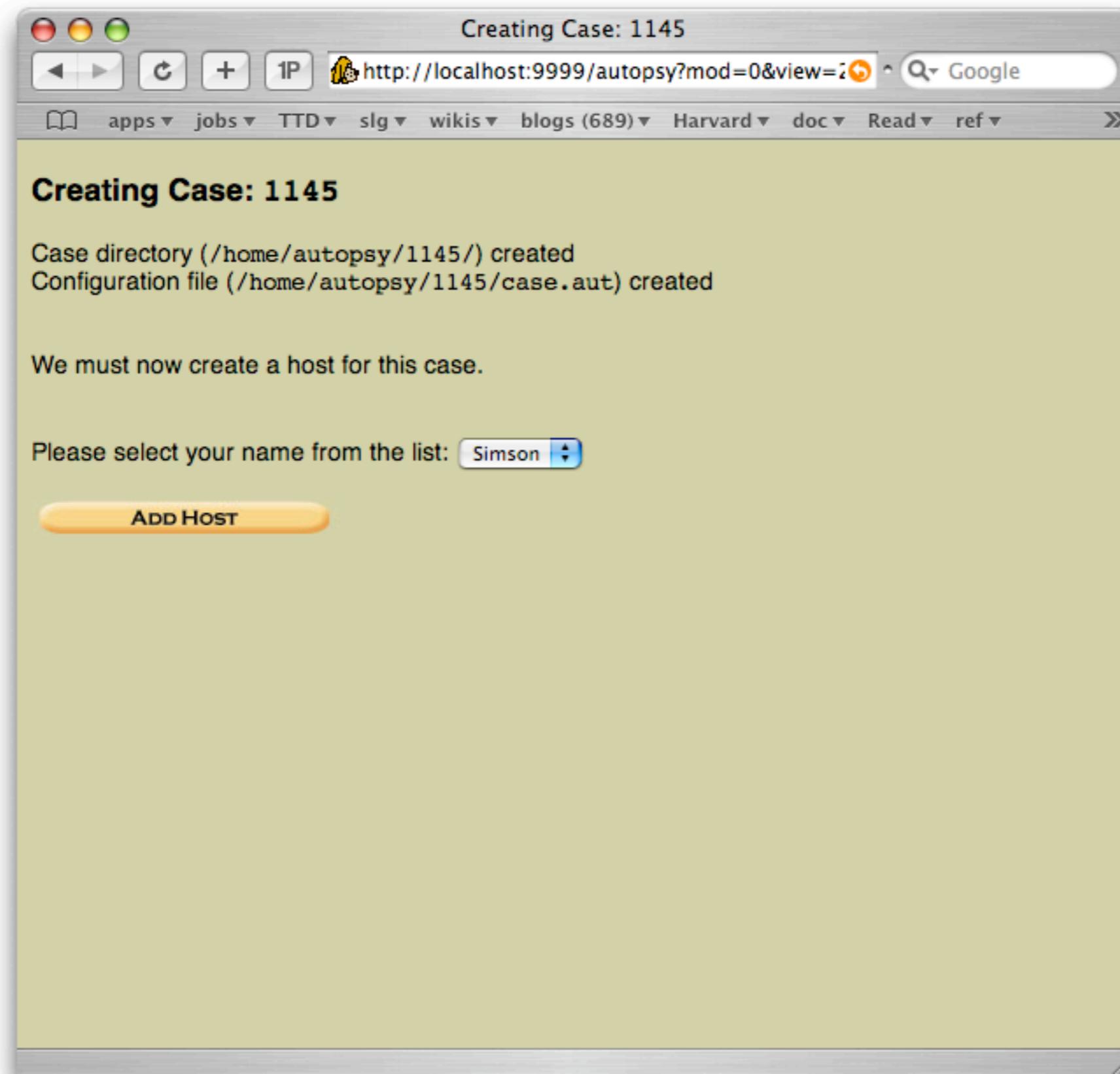
2. **Description:** An optional, one line description of this case.

1145

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a.	Simson	b.	
c.		d.	
e.		f.	
g.		h.	
i.		j.	

NEW CASE CANCEL HELP



Add A New Host To 1145

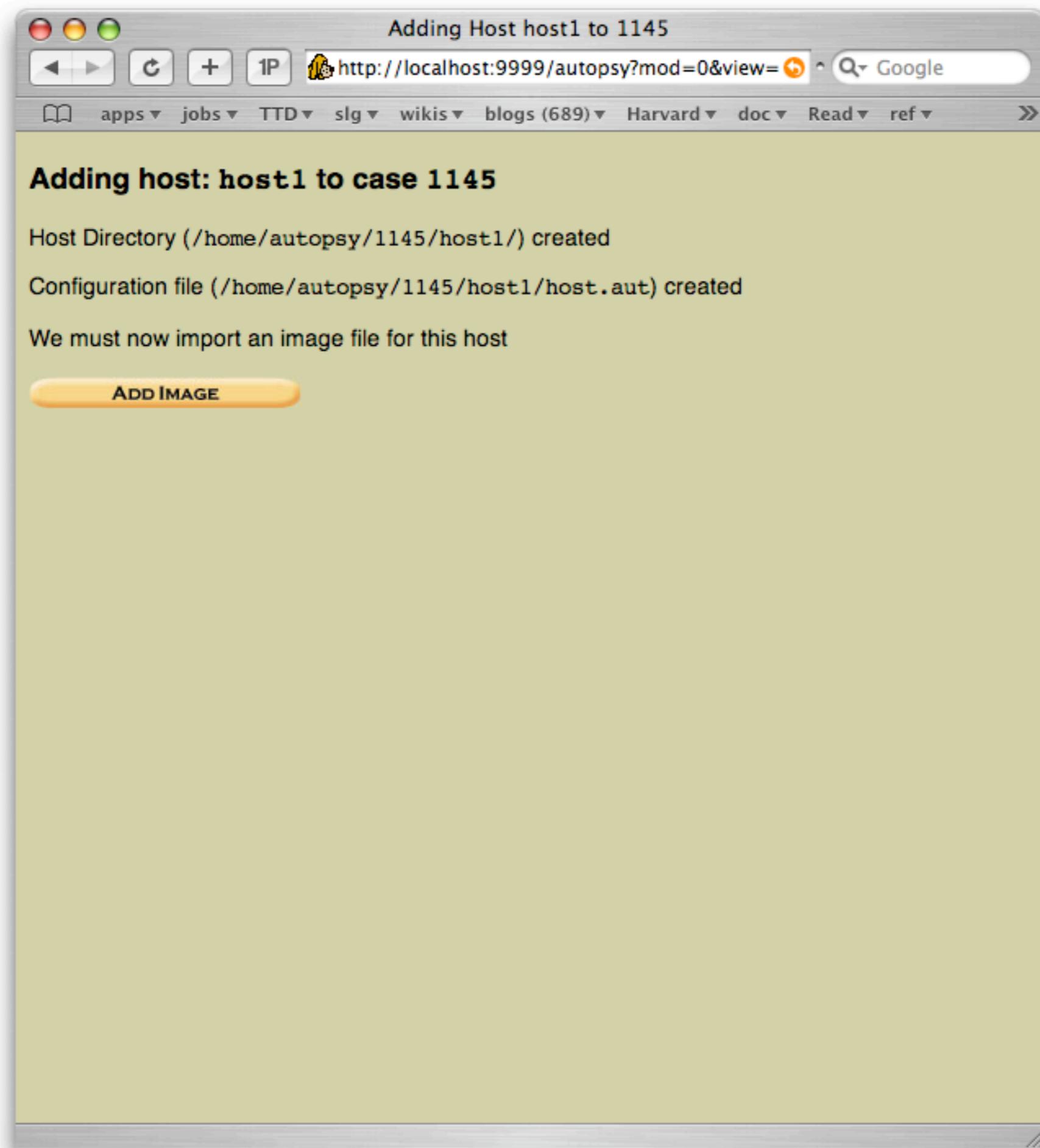
http://localhost:9999/autopsy?mod=0&view= Google

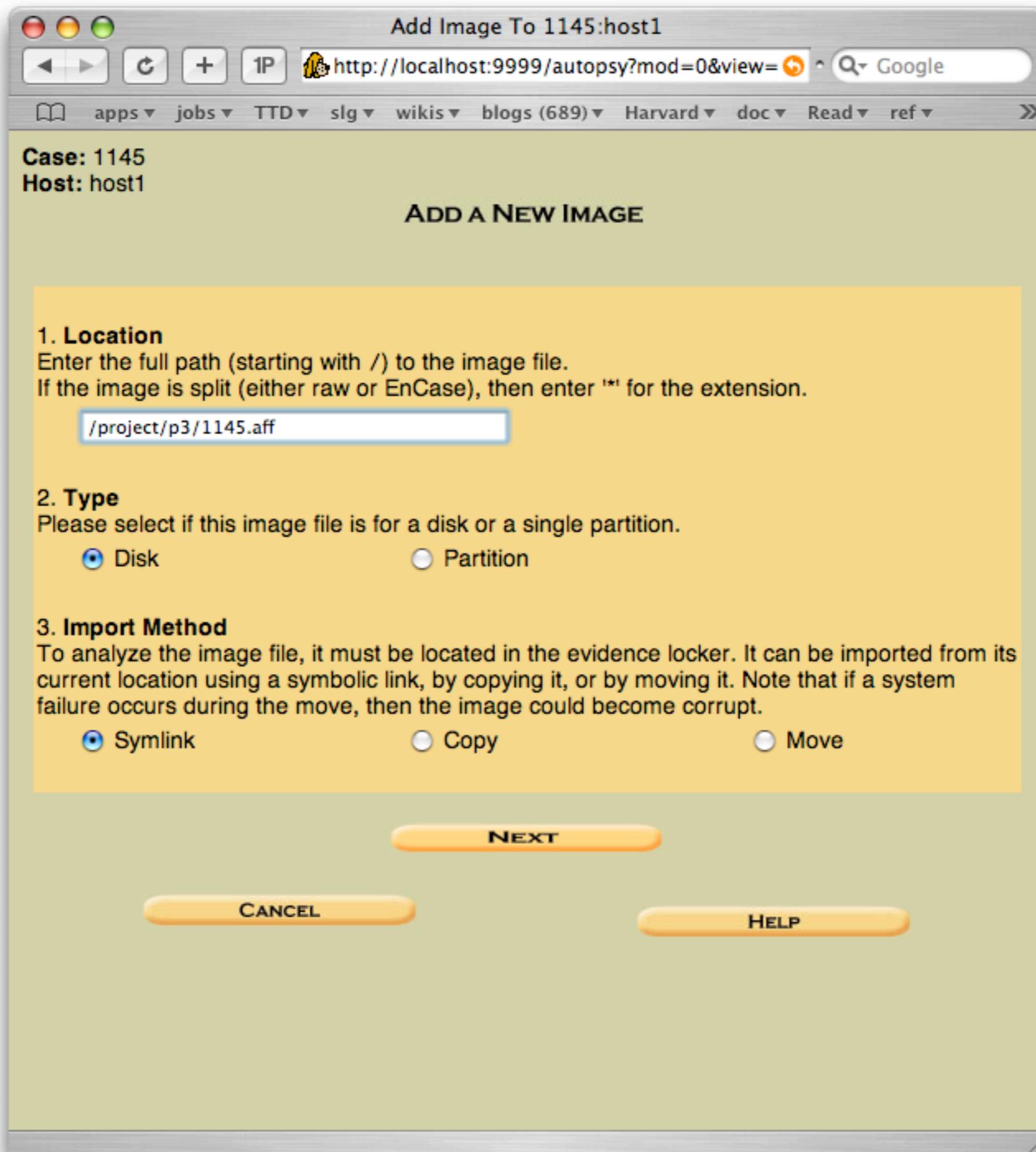
apps jobs TTD slg wikis blogs (689) Harvard doc Read ref

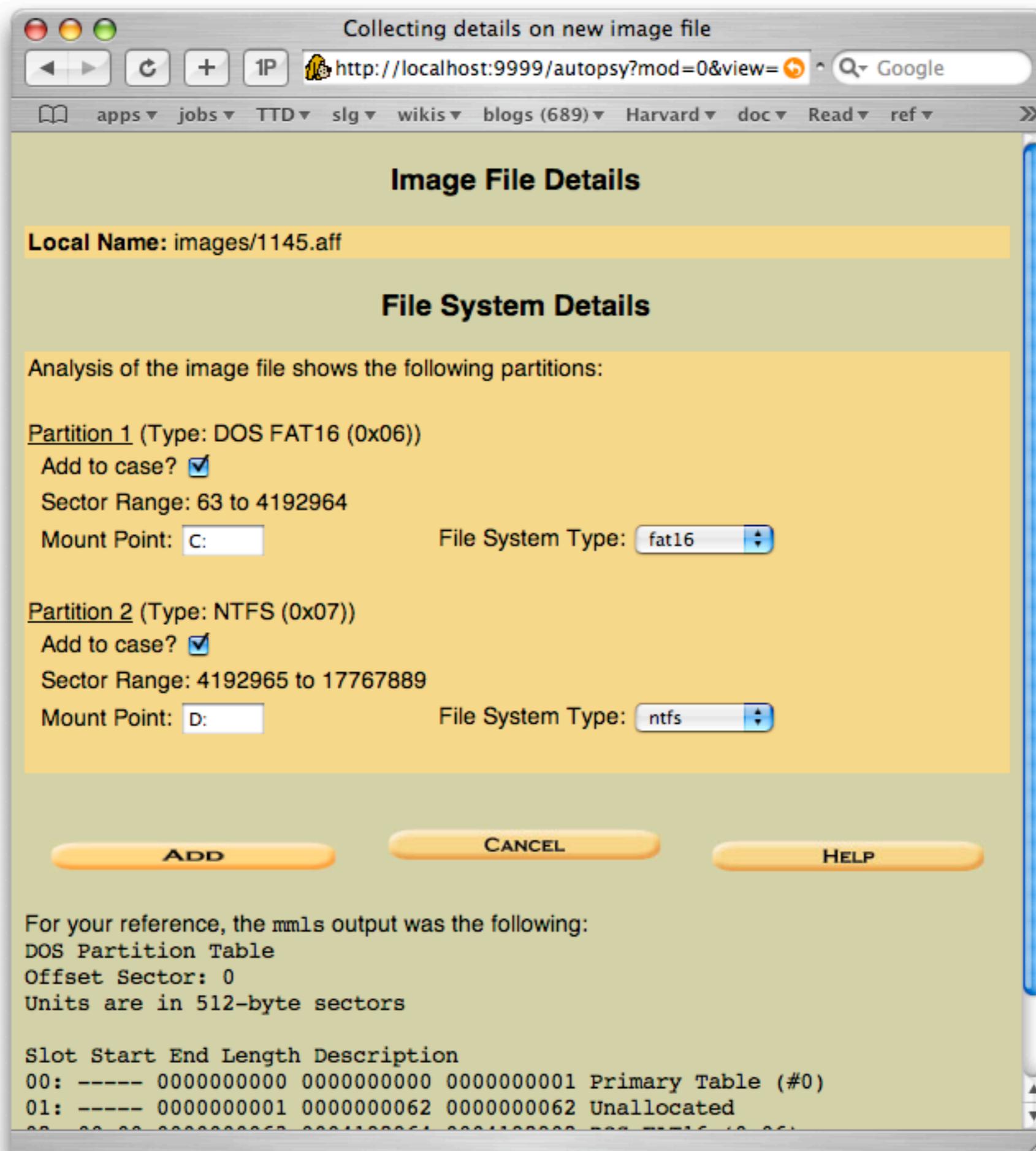
Case: 1145

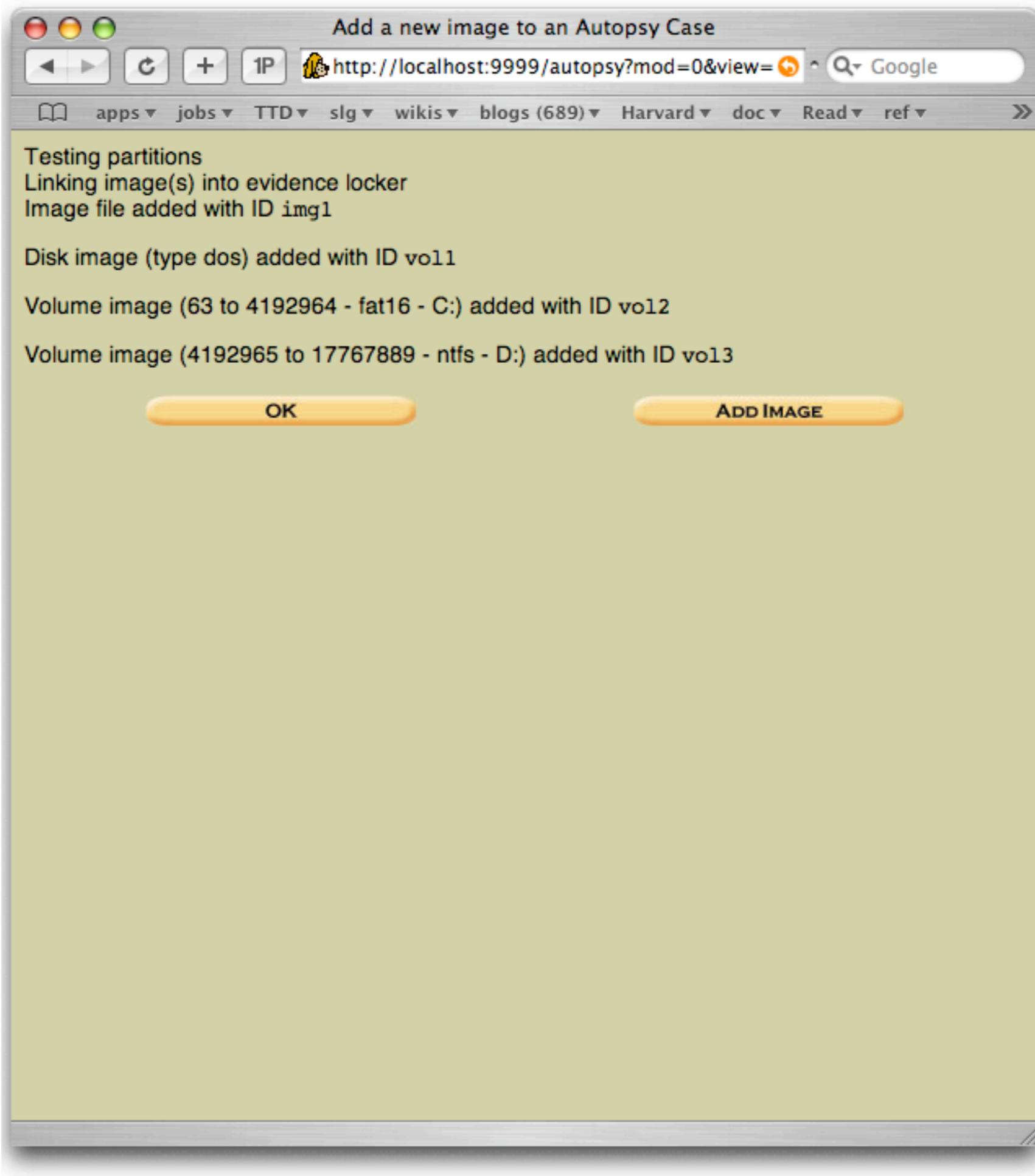
ADD A NEW HOST

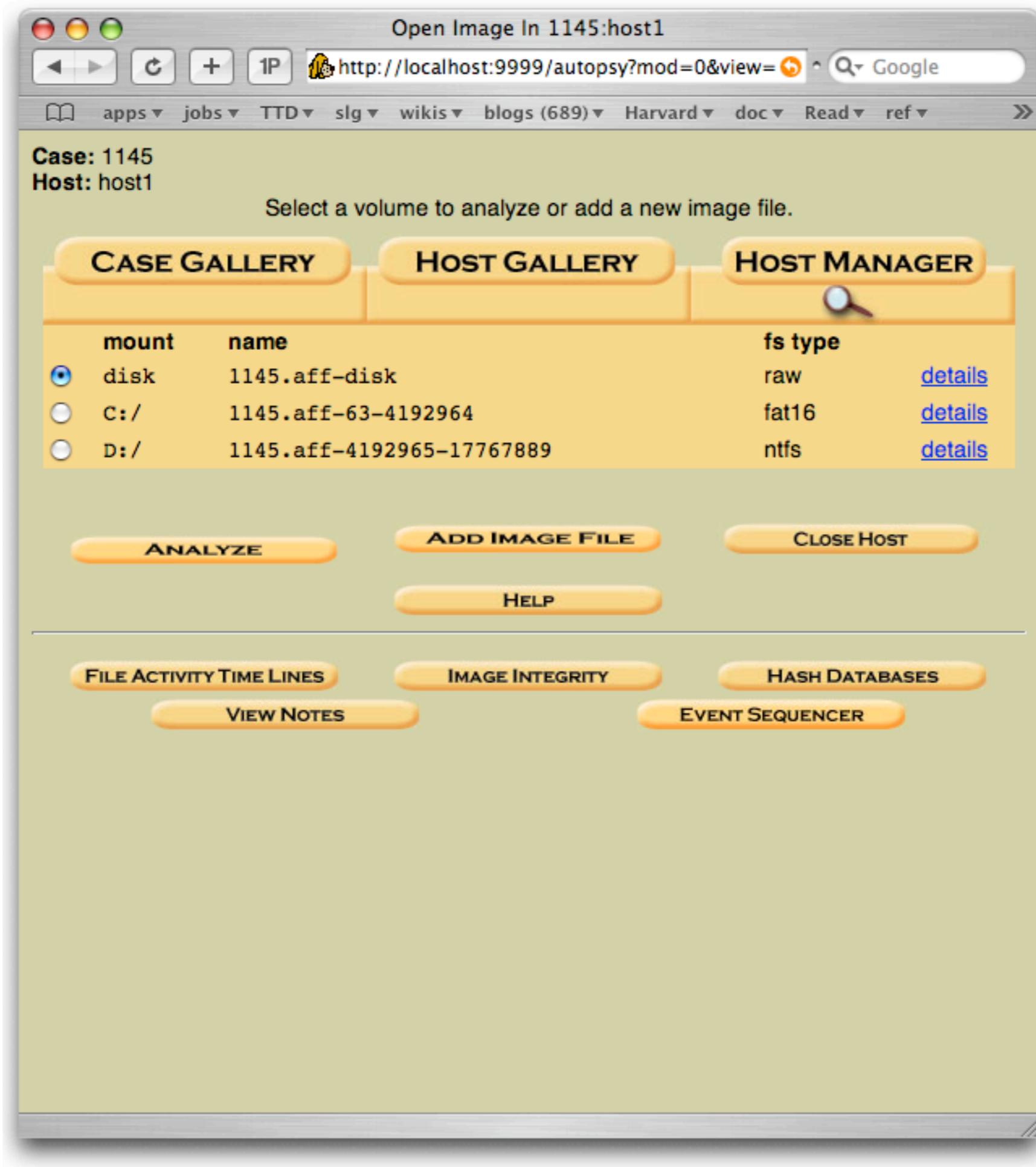
- 1. Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.
- 2. Description:** An optional one-line description or note about this computer.
- 3. Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.
- 4. Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.
- 5. Path of Alert Hash Database:** An optional hash database of known bad files.
- 6. Path of Ignore Hash Database:** An optional hash database of known good files.











1145:host1:vol2

http://localhost:9999/autopsy?mod=1&subm...

Google

apps jobs TTD slg wikis blogs (689) Harvard doc Read ref

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA

Directory Seek

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

C: /

VIEW

File Name Search

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

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES

✓	r / r	_w23.tmp	2001.09.05 14:18:14 (EDT)	2001.0
✓	r / r	_w23.tmp	2001.10.11 15:05:30 (EDT)	2001.1
✓	r / r	_w23.tmp	2001.10.11 15:06:32 (EDT)	2001.1
✓	r / r	_w26.tmp	2000.06.14 15:19:08 (EDT)	2000.0
✓	r / r	_w26.tmp	2000.06.14 23:14:56 (EDT)	2000.0
✓	r / r	_w26.tmp	2001.07.03 13:45:08 (EDT)	2001.0
✓	r / r	_w26.tmp	2001.07.03 13:45:26 (EDT)	2001.0

File Browsing Mode

In this mode, you can view file and directory contents.

File contents will be shown in this window.
More file details can be found using the Metadata link at the end of the list (on the right).
You can also sort the files using the column headers

1145:host1:vol2

http://localhost:9999/autopsy?mod=1&subm...

Google

apps jobs TTD slg wikis blogs (689) Harvard doc Read ref

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA

Directory Seek

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

C: /

VIEW

File Name Search

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

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES

r / r	SYSLEVEL.IBM	1999.12.09 02:37:18 (EST)	2001.1 00:00:
r / r	SYSLEVEL.IBM	1999.12.09 02:37:18 (EST)	2001.1 00:00:
d / d	TEMP/	2001.02.23 11:20:14 (EST)	2001.0 00:00:
d / d	ViaVoice/	2000.03.08 13:31:20 (EST)	2000.0 00:00:
d / d	WELCOME/	1999.12.09 02:50:56 (EST)	1999.1 00:00:
✓ d / d	Windows Update Setup Files/	2001.02.01 13:16:50 (EST)	2001.0 00:00:
d / d	WINNT40/	1999.12.09 02:43:00 (EST)	1999.1 00:00:
✓ r / r	Workshop dir	2000.03.03	2001.1

ASCII ([display](#) * [Hex](#) ([display](#) * [ASCII Strings](#) ([display](#) - [report](#)) * [Export](#) * [Add Note](#) - [report](#))

File Type: ASCII text, with CRLF line terminators

Contents Of File: C:/SYSLEVEL.IBM

```

CQHARUS
*****
CP31CUS
CP32BUS
CP34FUS
CQA002A
CQA004A
CQAC10A
CQB002A
CORR01A

```

Open "http://localhost:9999/autopsy?mod=2&view=8&cas...r=%2FSYSLEVEL.IBM&dirmode=2&recmode=0" in a new tab

Live CDs

Bootable CDRoms combine Linux + Forensic tools

- Lnx 4n6 - <http://www.lnx4n6.be/>
- The Farmer's Boot CD - <http://www.forensicbootcd.com/>
- Helix - <http://www.e-fense.com/helix>

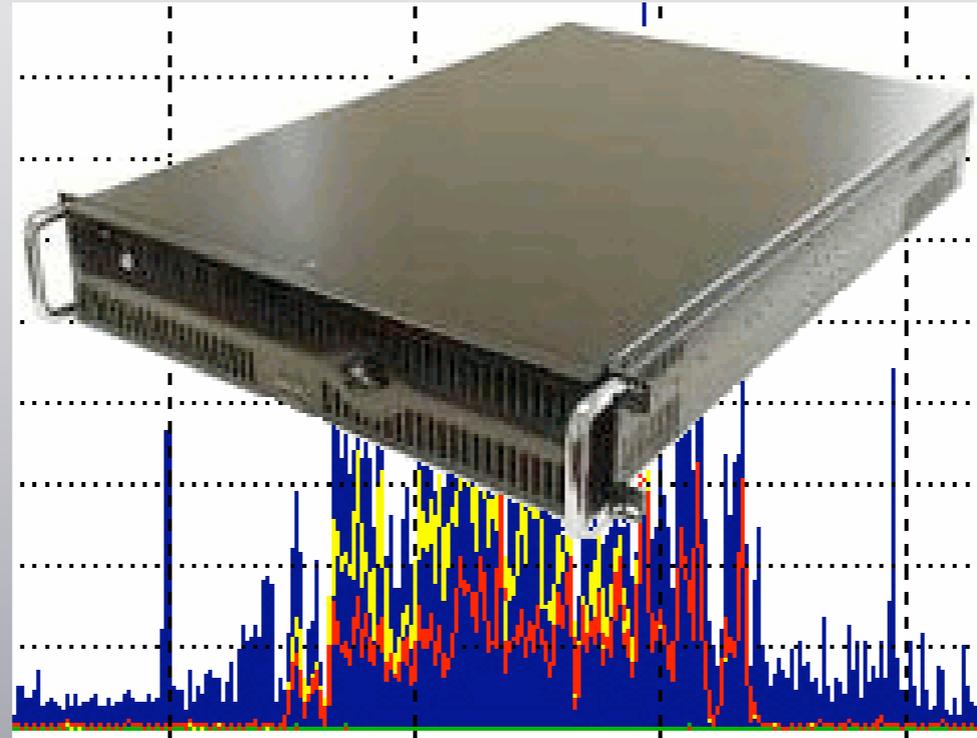
Advantages:

- No need to acquire hard drive

Dangers:

- Not all Linux distributions are forensically sound! Be careful!
- Some Linux distros will swap on the hard drive

Complete list at http://www.forensicswiki.org/wiki/Category:Live_CD



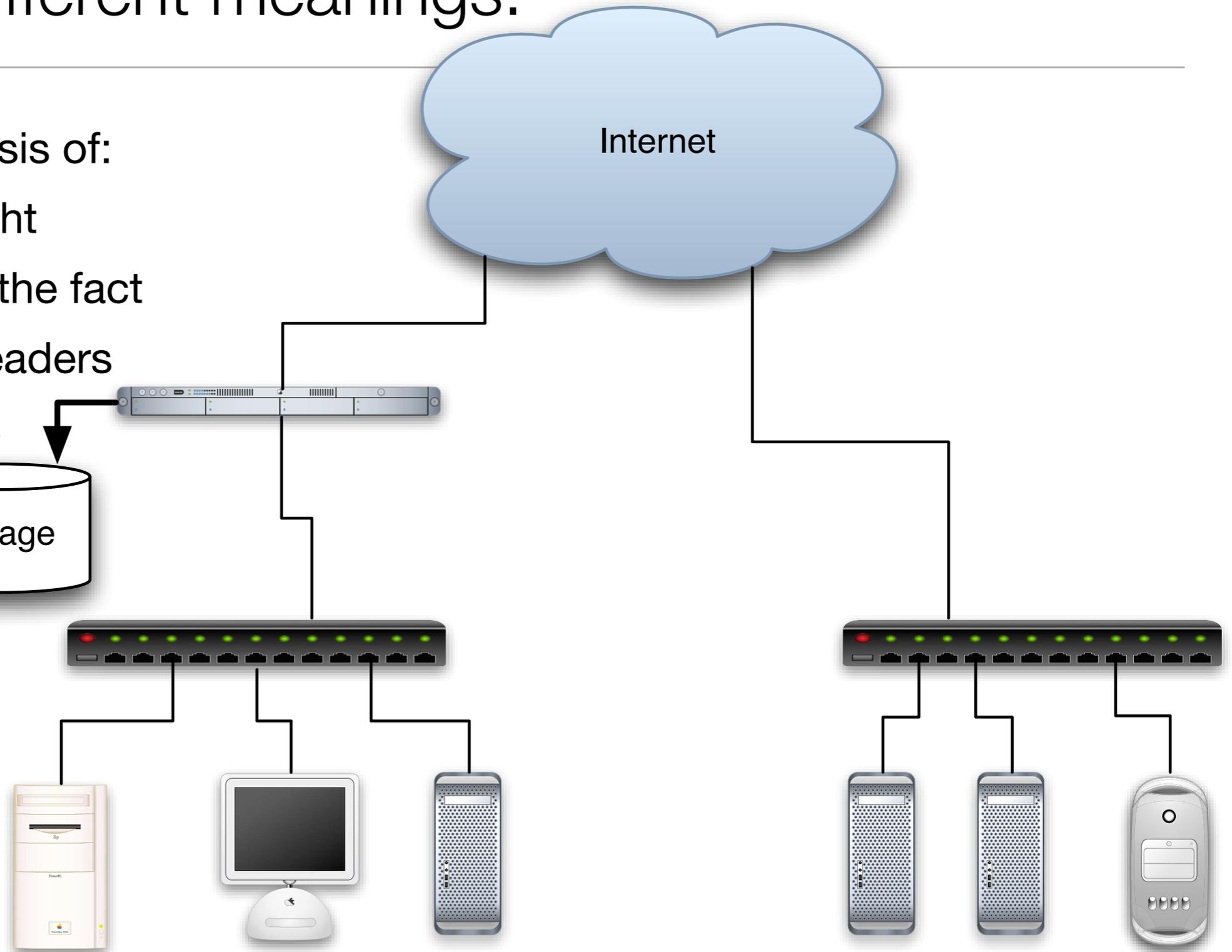
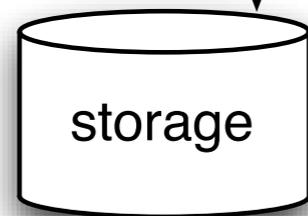
Network Forensics

packets
flows
logfiles

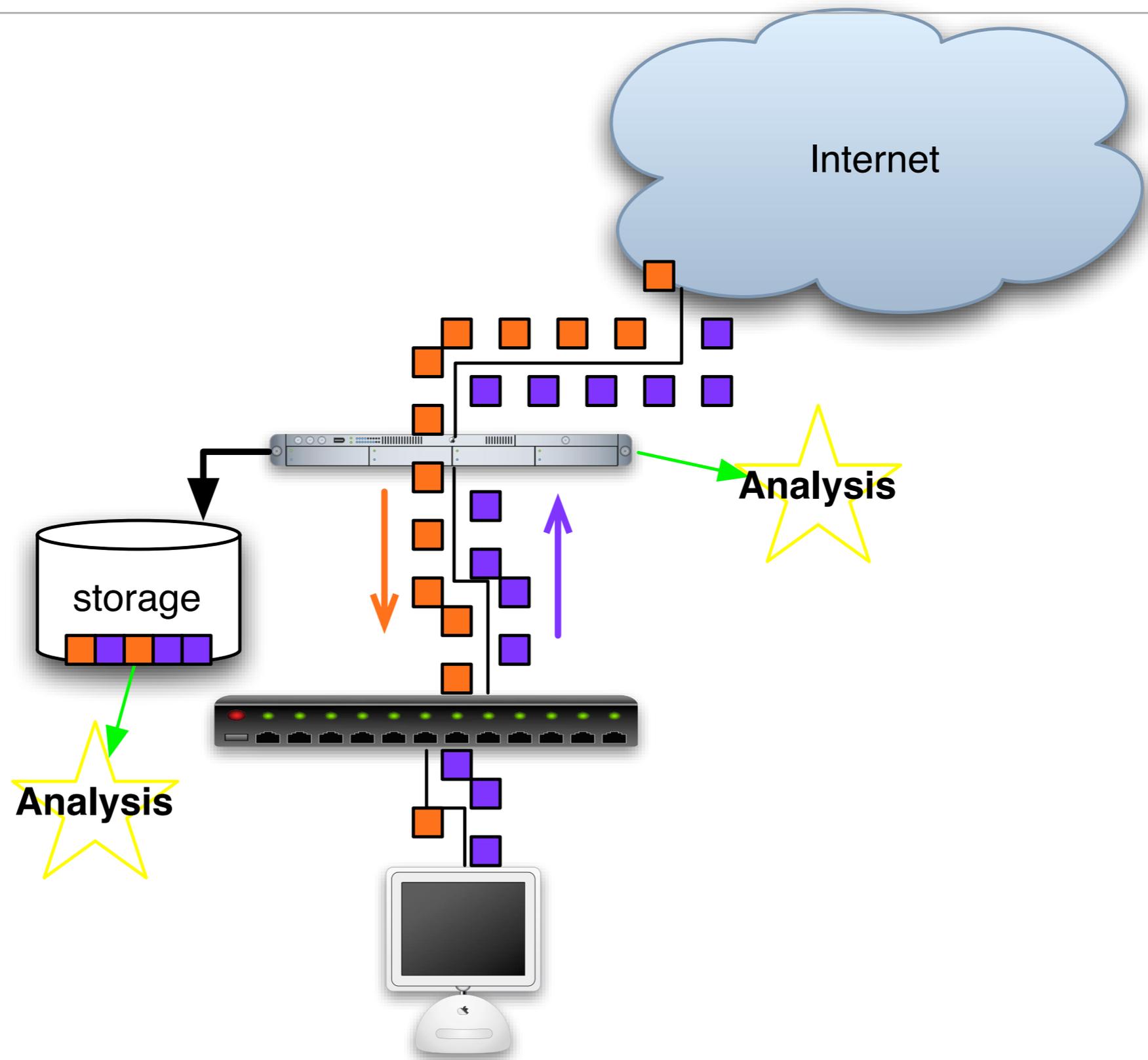
“Network Forensics” has many different meanings.

Capture and Analysis of:

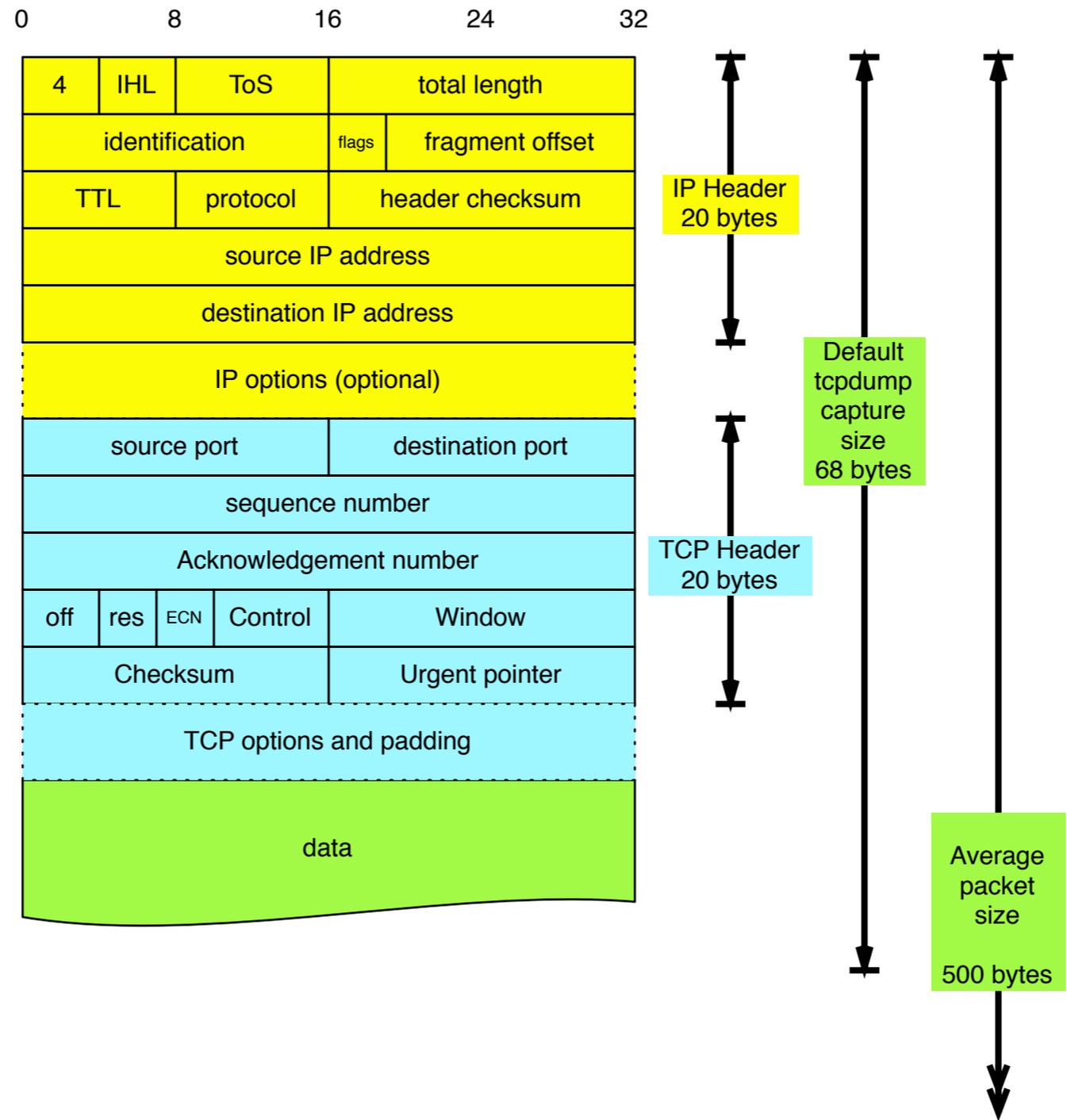
- packets in flight
- packets after the fact
- just packet headers
- network flows
- log files



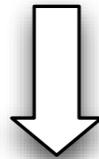
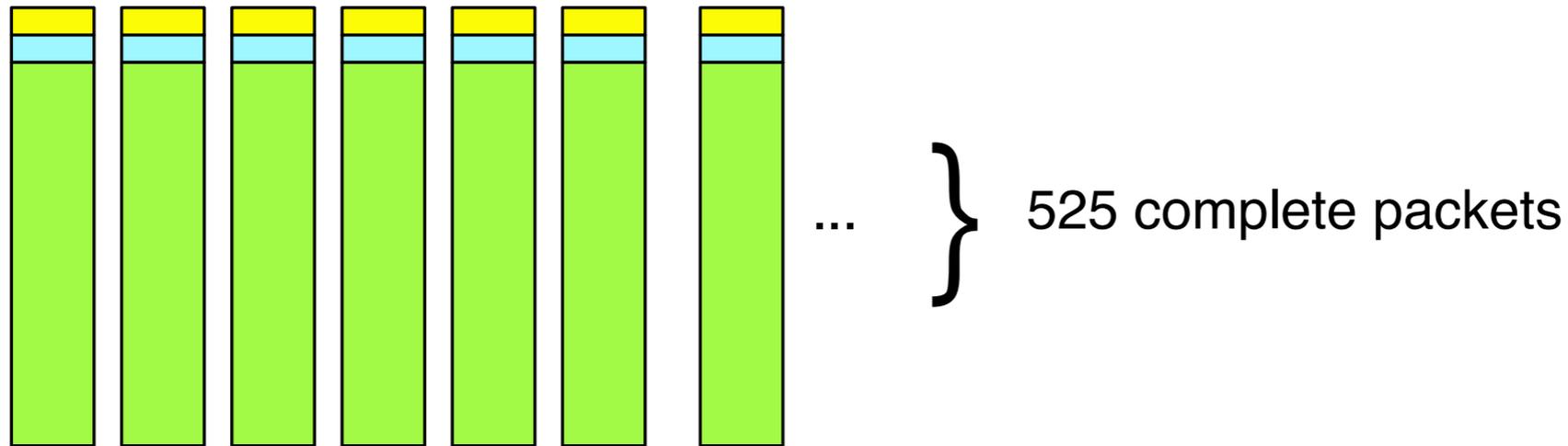
Packets can be analyzed in flight or after capture.



Systems can capture the *entire packet* or *just the packet header*



Complete packets allows for reconstruction.



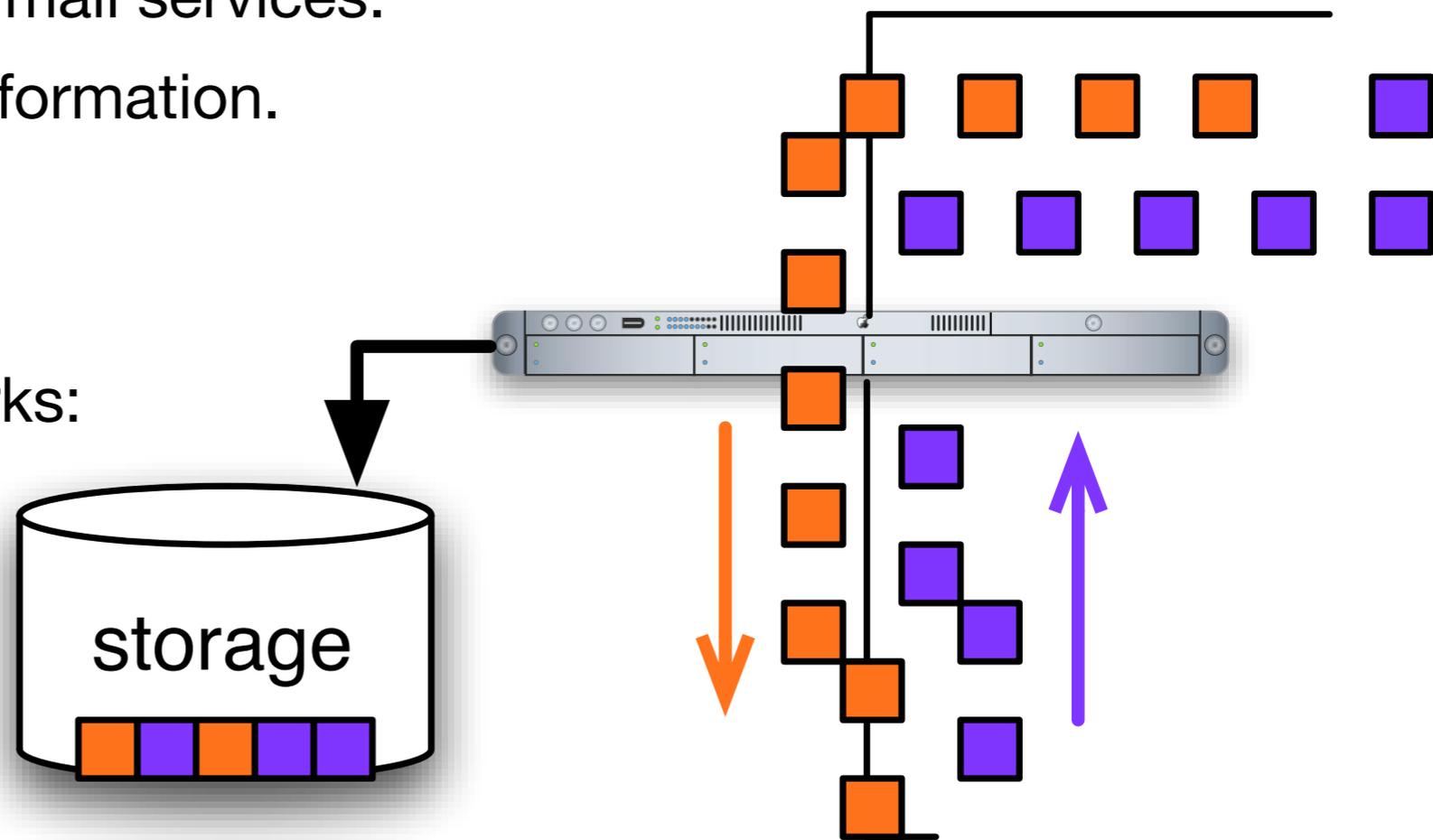
Some vendors call this “deep packet inspection” or “deep packet analysis.”

Primary use is to discover inappropriate data transfer or service use:

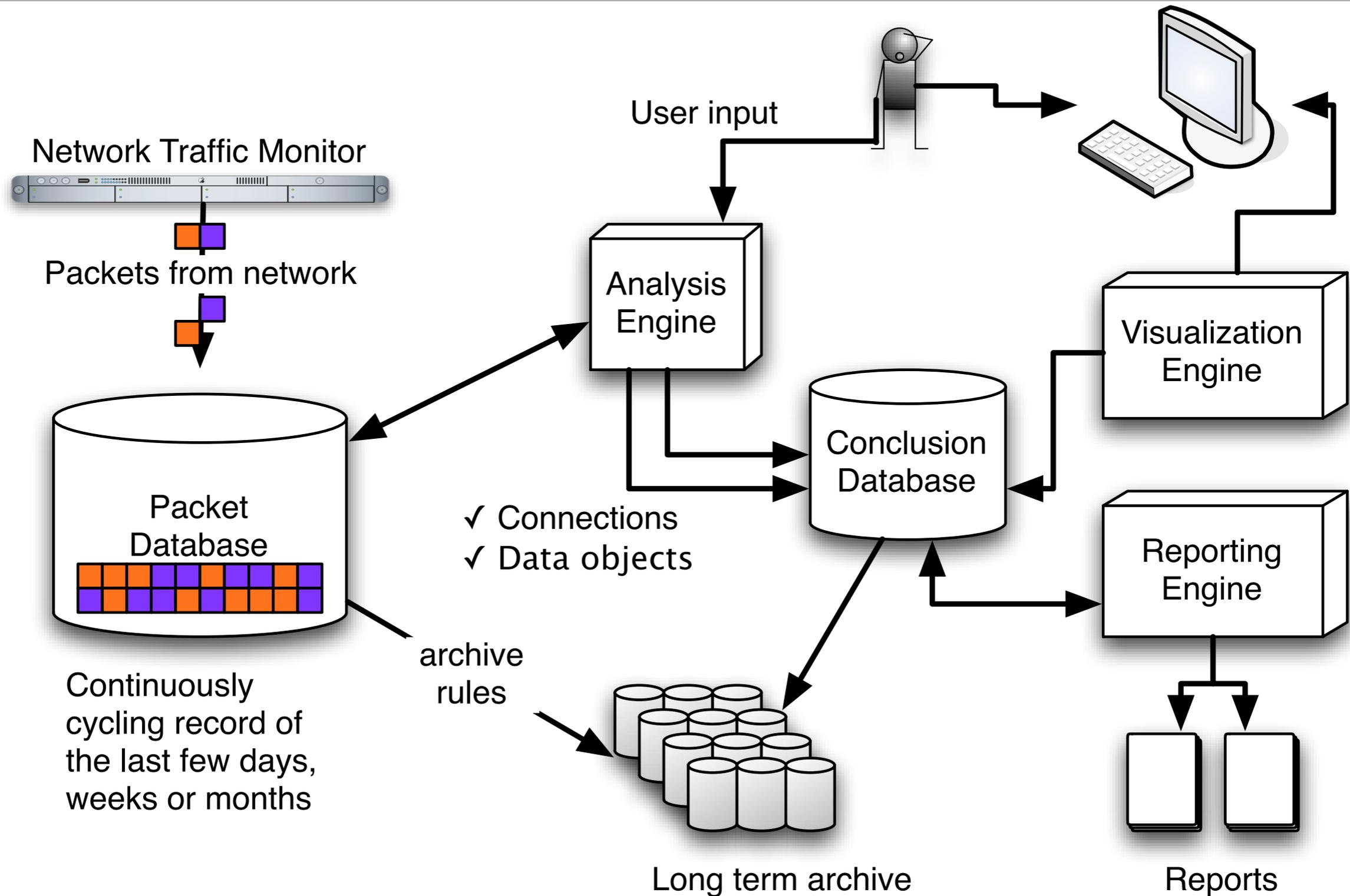
- Use of outside chat or web mail services.
- Leaking protected health Information.
- Restrict information

Also good for debugging networks:

- Duplicate requests
- Incomplete transactions
- Discovery of vulnerabilities without scanning
- Cleartext usernames & passwords



Network Forensics Architecture



Packet monitoring is similar to wiretapping.

Passive Monitoring Options:

- Use an ethernet “hub” with a packet sniffer.
- Set up a switched monitoring port.
- Full-duplex networks may require *two* monitoring ports.

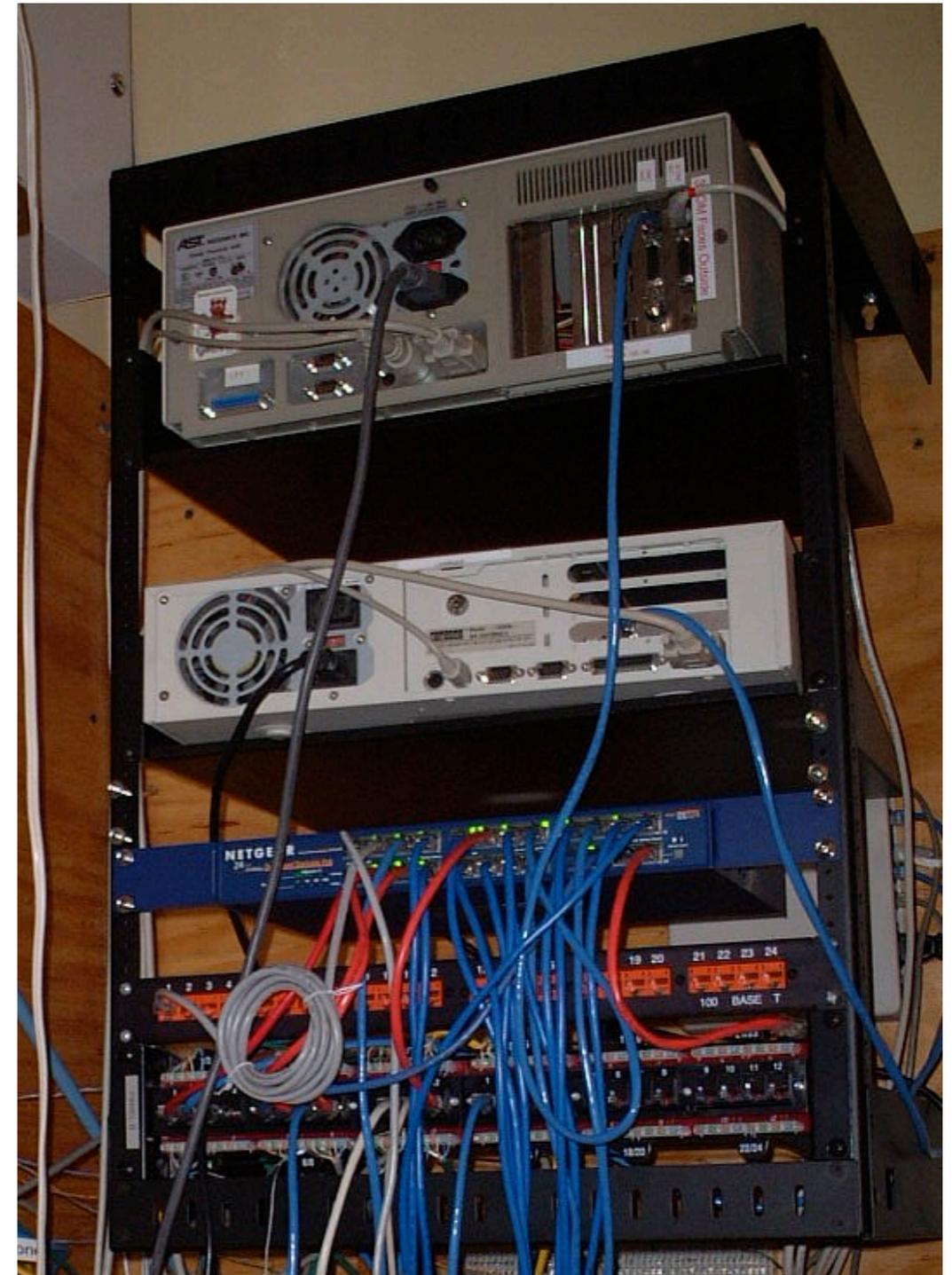
Active Monitoring Options:

- Monitor with a proxy or router.
- Monitor packets at endpoints

Critical uses:

- Attack assessment
- Policy enforcement

“A DVR for an Internet connection.”



Internet Wiretapping History

- 1983 — Netwatch – Graphical display of Internet Traffic
- 1990 — First reports of hostile packet sniffers
- 1995 — Ardita (Harvard FAS monitored by FBI)
- 1997 — FBI / DOJ / Carnivore
- 1999 — Emergence of commercial tools
- 2003 — Cisco Systems adds “Lawful Intercept Controls” to switches to allow eavesdropping on VoIP conversations “without detection”
- 2007 — FBI reportedly adopts large-scale Internet surveillance techniques.

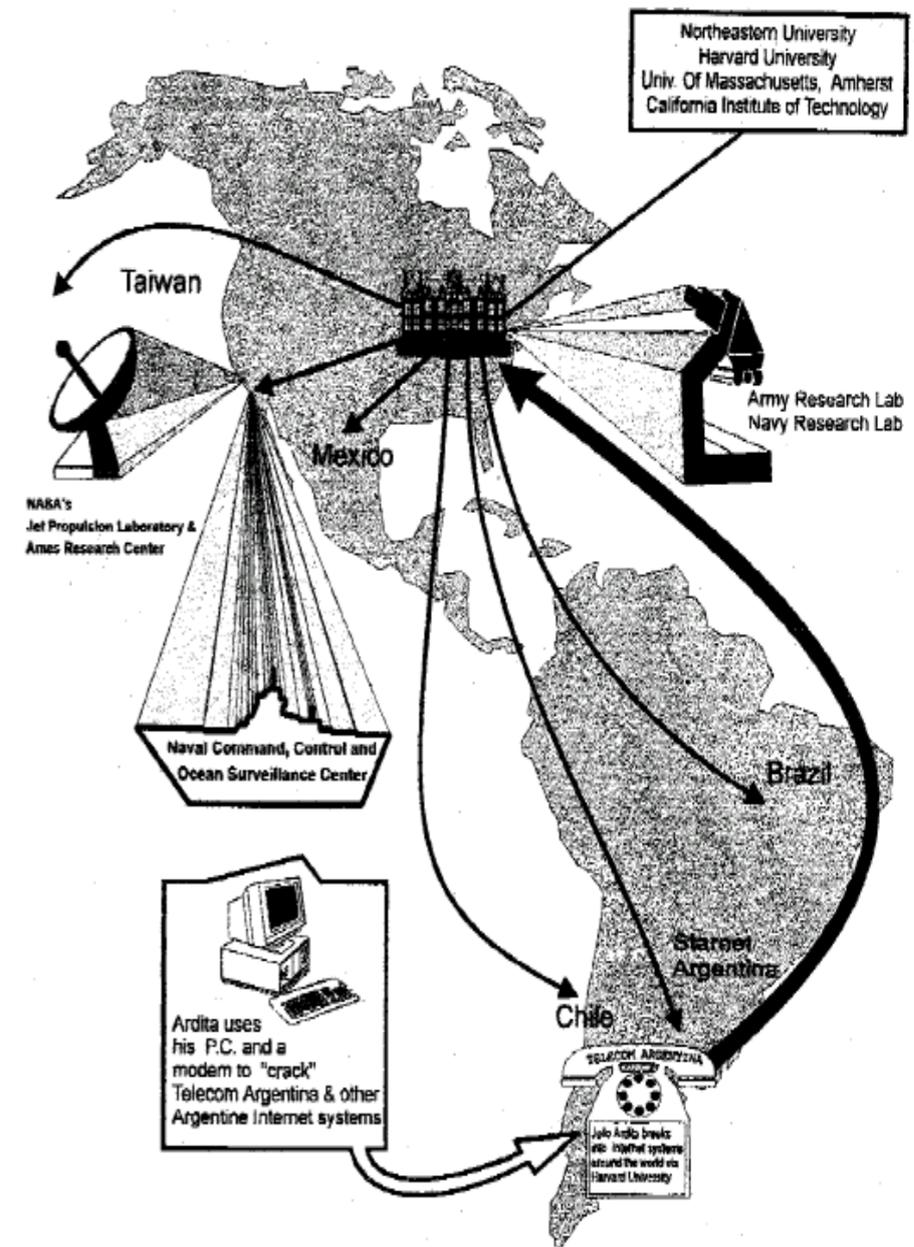
1996: Julio Caesar Ardita used Harvard FAS as a jump-off point

From Harvard, Ardita penetrated military and commercial systems throughout the world.

FBI installed TCP/IP stream reassembler with keyword trigger developed by US Army

Details at:

<http://www.simson.net/ref/1996/ardita.pdf>



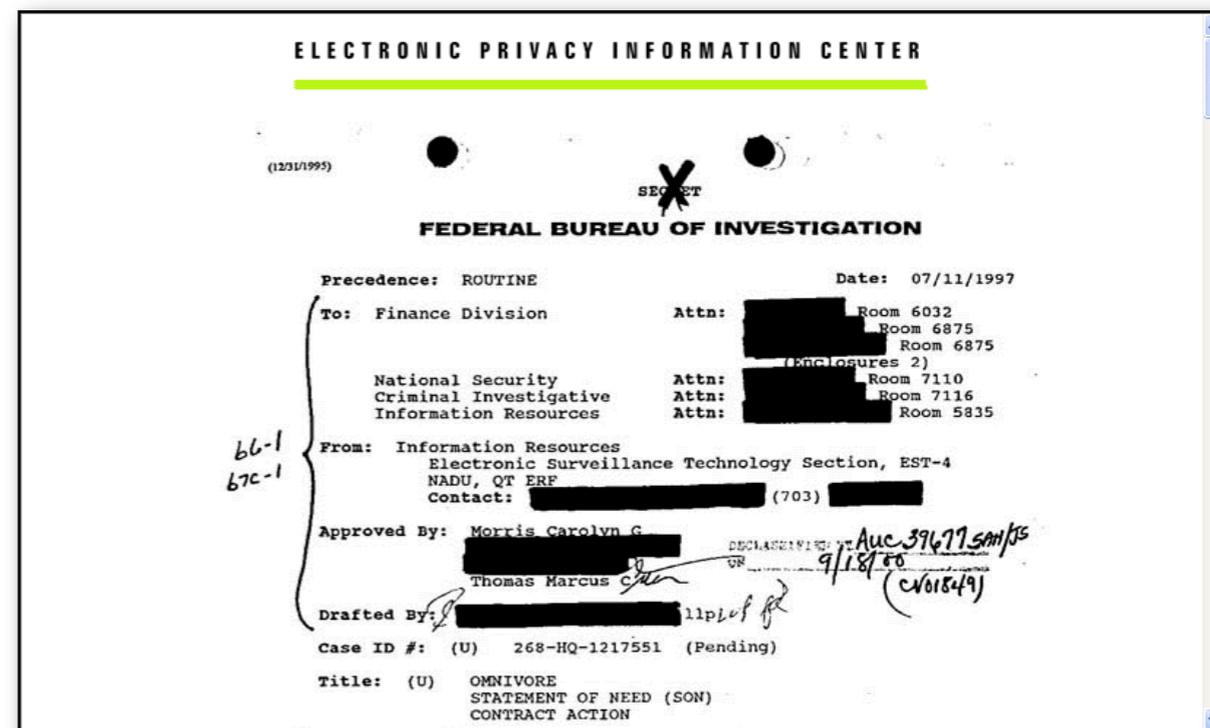
1997:

US Department of Justice develops “Omnivore”

Hodge-podge of technologies:

- Monitoring of IP and
■ ■ ■ ■ ■ ■ ■ ■ protocols
- Intercepts stored on ZIP disks
- Solaris X.86
- Triggers on:
 - SMTP username
 - RADIUS

\$2,315,000 development cost



<http://www.epic.org/privacy/carnivore/omnivoreproposal.html>

1998: Omnivore renamed “Carnivore” (“gets at the meat”)

Targeting Techniques:

- email usernames, RADIUS username
- IP address, DHCP mac address

Analysis:

- Logins & Logouts
- Email “pen register” (SMTP & RFC822)
- telnet

Apparently designed for medium-sized dial-up ISPs.

Renamed Digital Collection System 2000 (DSC2000)

Reportedly abandoned in favor of commercial and open source tools

Is it reasonable to capture all the packets?

In 1991, Los Alamos captured all information in and out of the lab's T1 on DAT tape:

- 8 gigabytes/day (50%)

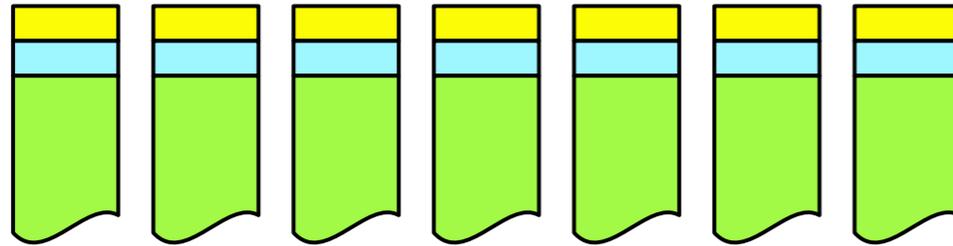
Disks have gotten bigger faster than network connections have gotten faster.

Connection	GB/Day (50%)
T1	8 GB
10 Mbit	54 GB
T3	170 GB
OC3	512 GB
OC12	2,000 GB

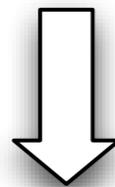
This is an engineering problem.

Once implemented, it can also be privacy problem.

With just headers, you can only get source, destination, size, timestamps, ports, etc.



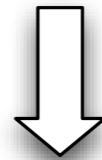
... } 525 packet headers



```
10:52:16.294858 IP 192.168.1.102.58754 > www2.cnn.com.http: S
10:52:16.370616 IP www2.cnn.com.http > 192.168.1.102.58754: S
10:52:16.370700 IP 192.168.1.102.58754 > www2.cnn.com.http: .
10:52:16.371114 IP 192.168.1.102.58754 > www2.cnn.com.http: P
10:52:16.455120 IP www2.cnn.com.http > 192.168.1.102.58754: .
10:52:19.956986 IP i7.cnn.net.http > 192.168.1.102.58755: .
10:52:19.961475 IP i7.cnn.net.http > 192.168.1.102.58755: .
10:52:19.981228 IP cnn1.dyn.cnn.com.http > 192.168.1.102.58766:
10:52:19.983731 IP cl4.cnn.com.http > 192.168.1.102.58761: P
```

Packet headers can be used to reconstruct “flows”

```
10:52:16.294858 IP 192.168.1.102.58754 > www2.cnn.com.http: S
10:52:16.370616 IP www2.cnn.com.http > 192.168.1.102.58754: S
10:52:16.370700 IP 192.168.1.102.58754 > www2.cnn.com.http: .
10:52:16.371114 IP 192.168.1.102.58754 > www2.cnn.com.http: P
10:52:16.455120 IP www2.cnn.com.http > 192.168.1.102.58754: .
10:52:19.956986 IP i7.cnn.net.http > 192.168.1.102.58755: .
10:52:19.961475 IP i7.cnn.net.http > 192.168.1.102.58755: .
10:52:19.981228 IP cnn1.dyn.cnn.com.http > 192.168.1.102.58766:
10:52:19.983731 IP cl4.cnn.com.http > 192.168.1.102.58761: P
```

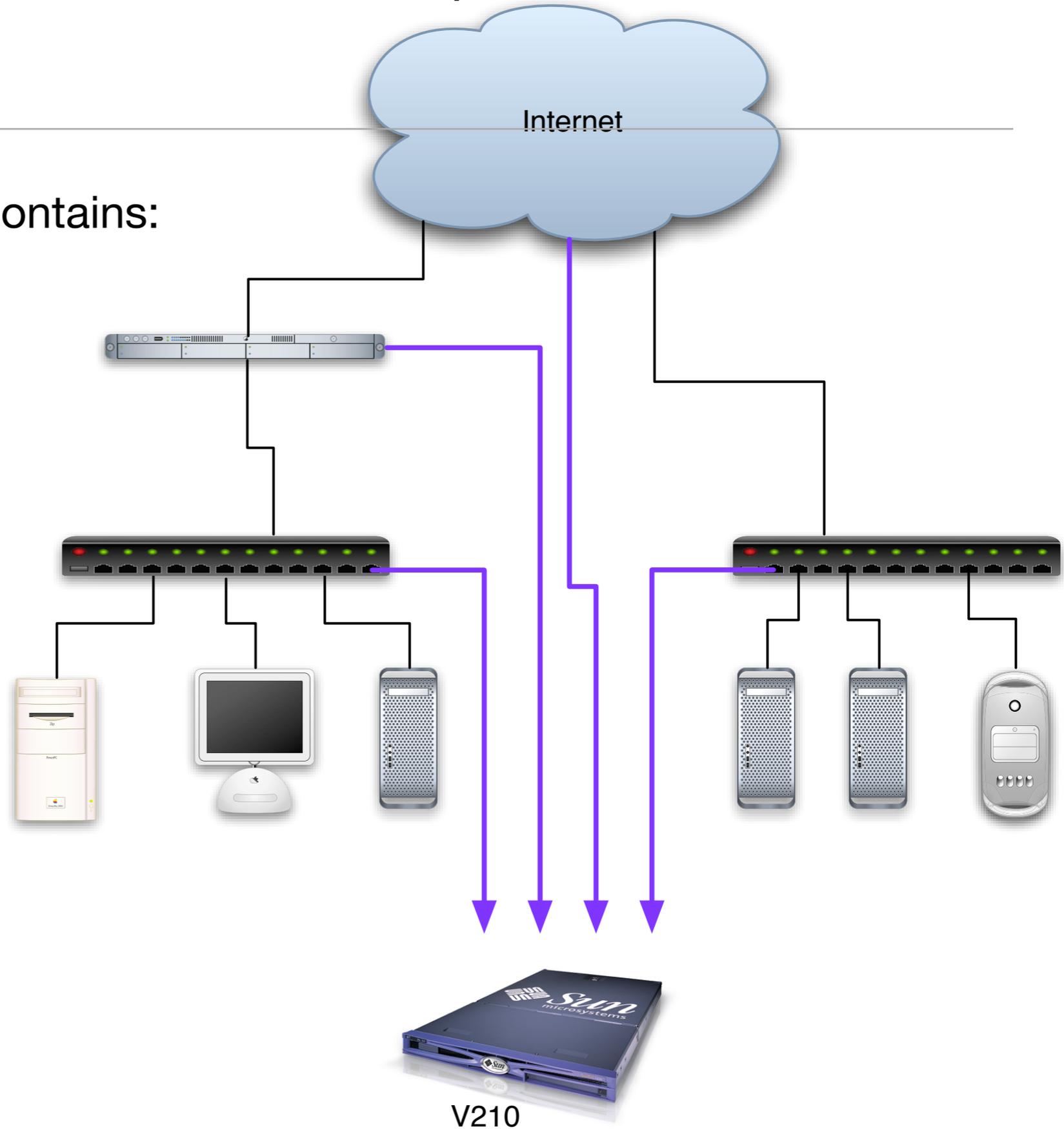


<u>Count</u>	<u>Source</u>	<u>></u>	<u>Destination</u>
46	i7.cnn.net.http	>	192.168.1.102.58755
34	192.168.1.102.58755	>	i7.cnn.net.http
26	69.22.138.51.http	>	192.168.1.102.58776
24	www2.cnn.com.http	>	192.168.1.102.58754
21	192.168.1.102.58776	>	69.22.138.51.http
19	192.168.1.102.58765	>	i7.cnn.net.http
17	64.236.29.63.http	>	192.168.1.102.58758
17	192.168.1.102.58754	>	www2.cnn.com.http
16	i7.cnn.net.http	>	192.168.1.102.58765
14	192.168.1.102.58759	>	64.236.29.63.http
13	72.32.153.176.http	>	192.168.1.102.58769
13	192.168.1.102.58769	>	72.32.153.176.http
13	192.168.1.102.58758	>	64.236.29.63.http
12	64.236.29.63.http	>	192.168.1.102.58759
10	64.236.29.63.http	>	192.168.1.102.58778
10	64.236.29.63.http	>	192.168.1.102.58757

Many switches and routers will report “netflow” data directly.

Each Cisco NetFlow record contains:

- Total bytes & packets
- S&D IP addresses
- S&D ports (UDP or TCP)
- flags
- start & end time
- min & max packet size
- VLANs & ifaces
- Vendor proprietary data



Flow data can still be a privacy problem

Flow data can reveal:

- When somebody went to work, left for home, etc.
- Which websites a person visited (but not perfectly).
- Applications that were used.

Flow data can be readily combined with other information:

- RADIUS / DHCP logs
- Mail logs

Each computer and router generates log files. Here's what's on my MacBook:

Date & Time of:

- OS installation
- Calendar syncs
- Wake from sleep & time slept
- Every program that crashed
- Every file installed
- Every log-in and log-out

Other information:

- Daily amount of free space
- Every 802.11 network found
- Every associated network



Apple's Wi-Fi Logs reveal where the laptop has been...

```
2007.05.07 21:05:50 Could not find "Harvard University" on channel(s) 1] [Level 4] [UID -2] [GID -2] [Host Black]
2007.05.07 21:05:50 Could not find "loganwifi" on channel(s) 11 1] [Level 4] [UID -2] [GID -2] [Host Black]
2007.05.07 21:05:50 Already scanned channels 11 for "CFP03"; not found.] [Level 4] [UID -2] [GID -2] [Host Black]
2007.05.07 21:05:51 Could not find "CFP01" on channel(s) 6] [Level 4] [UID -2] [GID -2] [Host Black]
2007.05.07 21:05:51 Already scanned channels 1 for "Data Surveillance"; not found.] [Level 4] [UID -2] [GID -2]
[Host Black]
2007.05.07 21:05:51 Already scanned channels 6 for "Hilton Bonaventure WiFi"; not found.] [Level 4] [UID -2] [GID
-2] [Host Black]
2007.05.07 21:05:51 Already scanned channels 1 for "CFP02"; not found.] [Level 4] [UID -2] [GID -2] [Host Black]
2007.05.07 21:05:52 No networks found on channel(s) 4] [Level 4] [UID -2] [GID -2] [Host Black]
2007.05.07 21:05:52 Could not find "STMnet-public" on channel(s) 4] [Level 4] [UID -2] [GID -2] [Host Black]
2007.05.07 21:05:52 Already scanned channels 11 for "espace"; not found.] [Level 4] [UID -2] [GID -2] [Host
Black]
2007.05.07 21:05:52 No networks found on channel(s) 11 6 1 36] [Level 4] [UID -2] [GID -2] [Host Black]
2007.05.07 21:05:52 Could not find "tmobile" on channel(s) 11 6 1 36] [Level 4] [UID -2] [GID -2] [Host Black]
2007.05.07 21:05:54 broadcast scan also didn't yield any matching result..] [Level 4] [UID -2] [GID -2] [Host
Black]
2007.05.07 21:06:31 Could not find "Harvard University" on channel(s) 1] [Level 4] [UID -2] [GID -2] [Host Black]
2007.05.07 21:06:32 Could not find "loganwifi" on channel(s) 11 1] [Level 4] [UID -2] [GID -2] [Host Black]
2007.05.07 21:06:32 Already scanned channels 11 for "CFP03"; not found.] [Level 4] [UID -2] [GID -2] [Host Black]
2007.05.07 21:06:32 Could not find "CFP01" on channel(s) 6] [Level 4] [UID -2] [GID -2] [Host Black]
2007.05.07 21:06:32 Already scanned channels 1 for "Data Surveillance"; not found.] [Level 4] [UID -2] [GID -2]
[Host Black]
2007.05.07 21:06:32 Already scanned channels 6 for "Hilton Bonaventure WiFi"; not found.] [Level 4] [UID -2] [GID
-2] [Host Black]
2007.05.07 21:06:32 Already scanned channels 1 for "CFP02"; not found.] [Level 4] [UID -2] [GID -2] [Host Black]
2007.05.07 21:06:33 No networks found on channel(s) 4] [Level 4] [UID -2] [GID -2] [Host Black]
2007.05.07 21:06:33 Could not find "STMnet-public" on channel(s) 4] [Level 4] [UID -2] [GID -2] [Host Black]
2007.05.07 21:06:33 Already scanned channels 11 for "espace"; not found.] [Level 4] [UID -2] [GID -2] [Host
Black]
2007.05.07 21:06:33 No networks found on channel(s) 11 6 1 36] [Level 4] [UID -2] [GID -2] [Host Black]
```

Apple's "Disk Utility" log files show what CDRROMs have been burned...

May 12 20:25:27: Disk Utility started.

Burning Image "**topo_ak_hi.dmg**"

Checksumming **TOPO_AK_HI** (Apple_ISO : 0)...

TOPO_AK_HI (Ap: verified CRC32 \$5B03581D

verified CRC32 \$2E6A5263

Preparing data for burn

Opening session

Opening track

Writing track

Closing track

Closing session

Finishing burn

Verifying burn...

Verifying

Burn completed successfully

Image "**topo_ak_hi.dmg**" burned successfully.

Burning Image "**topo_us_west.dmg**"

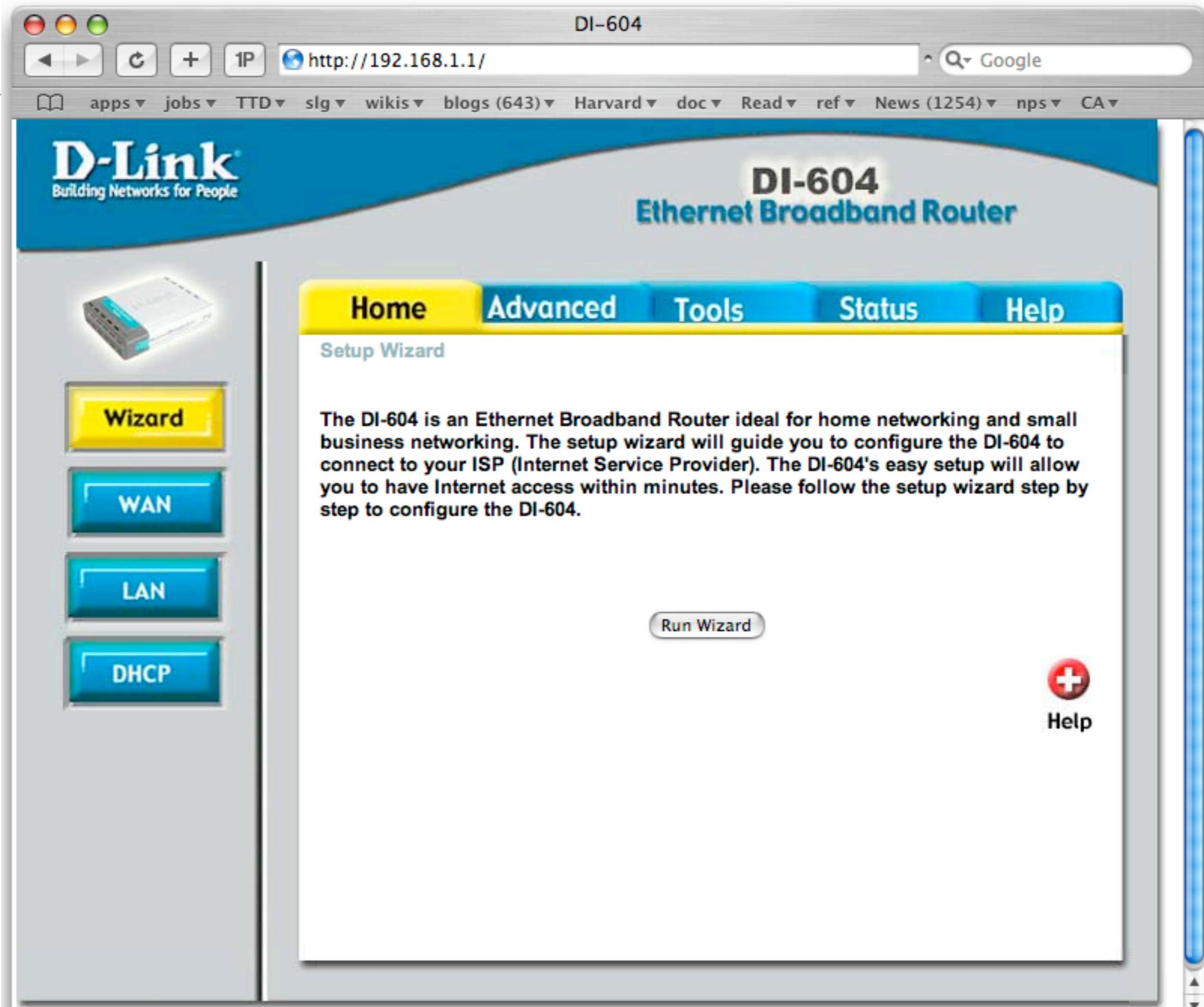
Checksumming **TOPO_US_WEST** (Apple_ISO : 0)...

TOPO_US_WEST (Ap: checksum canceled.

calculated CRC32 \$6BDCF6BA

Preparing data for burn

Even my home router keeps logs...



DI-604

http://192.168.1.1/st_devic.html

apps jobs TTD slg wikis blogs (643) Harvard doc Read ref News (1254) nps CA

D-Link
Building Networks for People

DI-604
Ethernet Broadband Router

Home Advanced Tools **Status** Help

Device Information

Firmware Version: 1.07DDM , Thu, 9 Dec 2004

LAN

MAC Address 00-11-95-2E-35-84

IP Address 192.168.1.1

Subnet Mask 255.255.255.0

DHCP Server Enabled

WAN

MAC Address 00-11-95-2E-35-85

Connection PPPoE Connected

IP Address 71.126.240.179

Subnet Mask 255.255.255.255

Default Gateway 71.126.240.179

DNS 71.243.0.12 71.250.0.12

Device Info

Log

Stats

 Help

DI-604

http://192.168.1.1/st_log.html

apps jobs TTD slg wikis blogs (643) Harvard doc Read ref News (1254) nps CA



Building Networks for People

DI-604

Ethernet Broadband Router

Home
Advanced
Tools
Status
Help

View Log
View Log displays the activities occurring on the DI-604. Click on Log Settings for advance features.


Help

First Page
Last Page
Previous
Next
Clear
Log Settings

page 1 of 17

Time	Message	SourceDestination	Note
May/12/2007 19:32:46	DHCP lease IP 192.168.1.108 to Sonias-iMac		00-0A-95-69-38-CC
May/12/2007 18:55:30	DHCP lease IP 192.168.1.105 to Black		00-16-CB-BF-89-D6
May/12/2007 18:55:28	DHCP lease IP 192.168.1.110 to Black		00-16-CB-CF-8F-5D
May/12/2007 16:50:52	DHCP lease IP 192.168.1.105 to Black		00-16-CB-BF-89-D6
May/12/2007 16:08:38	DHCP lease IP 192.168.1.108 to Sonias-iMac		00-0A-95-69-38-CC
May/12/2007 12:09:05	DHCP lease IP 192.168.1.108 to Sonias-iMac		00-0A-95-69-38-CC
May/12/2007 11:31:13	DHCP lease IP 192.168.1.104 to DELL		00-0D-56-08-E2-AF
May/12/2007 10:23:19	DHCP lease IP 192.168.1.108 to Sonias-iMac		00-0A-95-69-38-CC
May/12/2007 07:55:02	DHCP lease IP 192.168.1.102 to Elvis		00-13-02-23-EE-F1
May/11/2007 22:58:12	DHCP lease IP 192.168.1.106 to simsong		00-13-10-5C-A7-A4

Device Info

Log

Stats

DI-604

http://192.168.1.1/st_log.html

DI-604
Ethernet Broadband Router

D-Link
Building Networks for People

apps ▾ jobs ▾ TTD ▾ slg ▾ wikis ▾ blogs (643) ▾ Harvard ▾ doc ▾ Read ▾ ref ▾ News (1254) ▾ nps ▾ CA ▾

Home **Advanced** **Tools** **Status** **Help**

View Log
View Log displays the activities occurring on the DI-604. Click on Log Settings for advance features.



Device Info

Log

Stats

 **Help**

page 17 of 17

Time	Message	SourceDestination	Note
Apr/30/2007 00:00:33	DHCP lease IP 192.168.1.105 to Black		00-16-CB-BF-89-D6
Apr/30/2007 00:00:32	DHCP lease IP 192.168.1.110 to Black		00-16-CB-CF-8F-5D
Apr/29/2007 20:54:00	DHCP lease IP 192.168.1.100 to Airport-Extreme		00-03-93-DF-95-ED
Apr/29/2007 19:49:58	DHCP lease IP 192.168.1.106 to simsong		00-13-10-5C-A7-A4
Apr/29/2007 19:49:41	PPPoE line connected		
Apr/29/2007 19:49:40	WAN: Auto Dialup		Try to establish PPPoE line
Apr/29/2007 19:49:40	System started		
Apr/29/2007 19:49:36	pre_task		NVcfg_get, ret=0

DI-604

http://192.168.1.1/st_log_settings.html

apps jobs TTD slg wikis blogs (643) Harvard doc Read ref News (1254) nps CA

D-Link
Building Networks for People

DI-604
Ethernet Broadband Router

Home Advanced Tools **Status** Help



Device Info

Log

Stats

Log settings
Logs can be saved by sending it to an admin email address.

SMTP Server / IP Address

Email Address

Log Type

- System Activity
- Debug Information
- Attacks
- Dropped Packets
- Notice

Apply Cancel Help

DI-604

http://192.168.1.1/st_log_settings.html

apps jobs TTD slg wikis blogs (643) Harvard doc Read ref News (1254) nps CA

D-Link
Building Networks for People

DI-604
Ethernet Broadband Router

Home Advanced Tools **Status** Help



Device Info

Log

Stats

Log settings
Logs can be saved by sending it to an admin email address.

SMTP Server / IP Address: 140.247.60.24

Email Address: simsong@eecs.harvard.edu [Send Mail Now](#)

Log Type

- System Activity
- Debug Information
- Attacks
- Dropped Packets
- Notice

  
Apply Cancel Help

What can you do with activity logs?

Prosecution work:

- Show that a suspect was using a computer at a given time/place.
- Attempt to remove doubt.

Defense work:

- Show that a network was used by someone other than the suspect.
- Show that a computer was “asleep” when the crime was committed.
- Cast doubt.

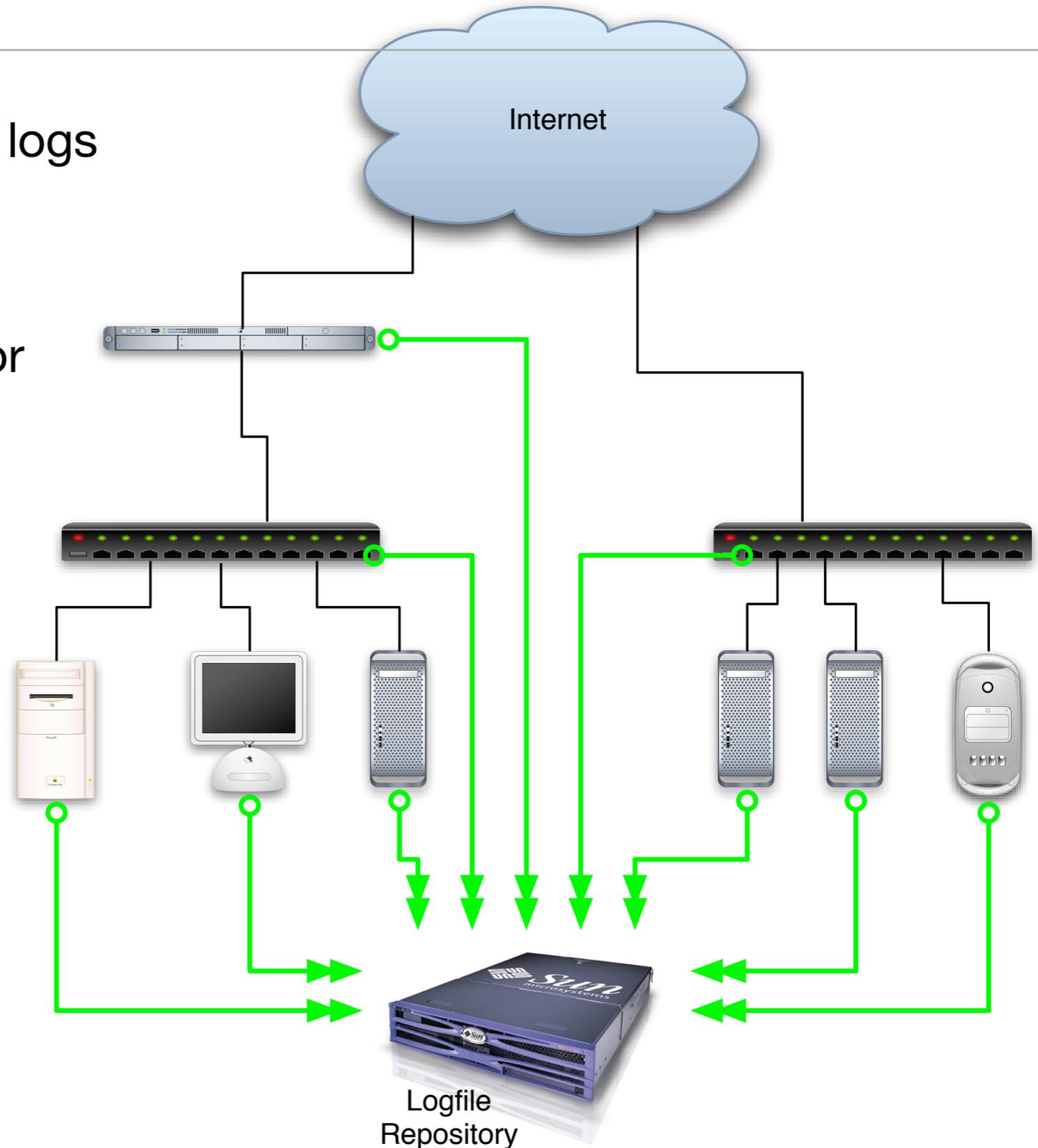
Remember: These logs can be faked, although they usually aren't.

(Of course, when they are brought forward by the relying party, they are more likely to be faked.)

Log files are kept on each host; they can be aggregated into a central location

A central repository makes the logs
more resistant to attack...

... and more subject to abuse or
covert access



Full-content “deep analysis” solutions:

Open Source

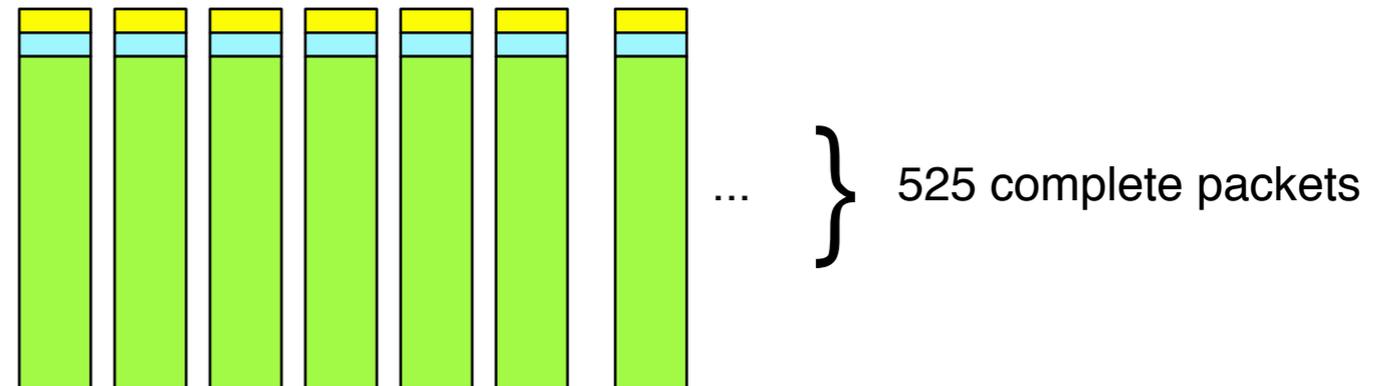
- Wireshark
- Snort
- Squil

Commercial in-memory:

- NFR
- Intrusic
- McAfee
- NetWitness

Commercial archiving systems:

- CA eTrust Network Forensics
- Chronicle Solutions
- NIKSUN NetDetector
- Sandstorm NetIntercept
- Network Intelligence



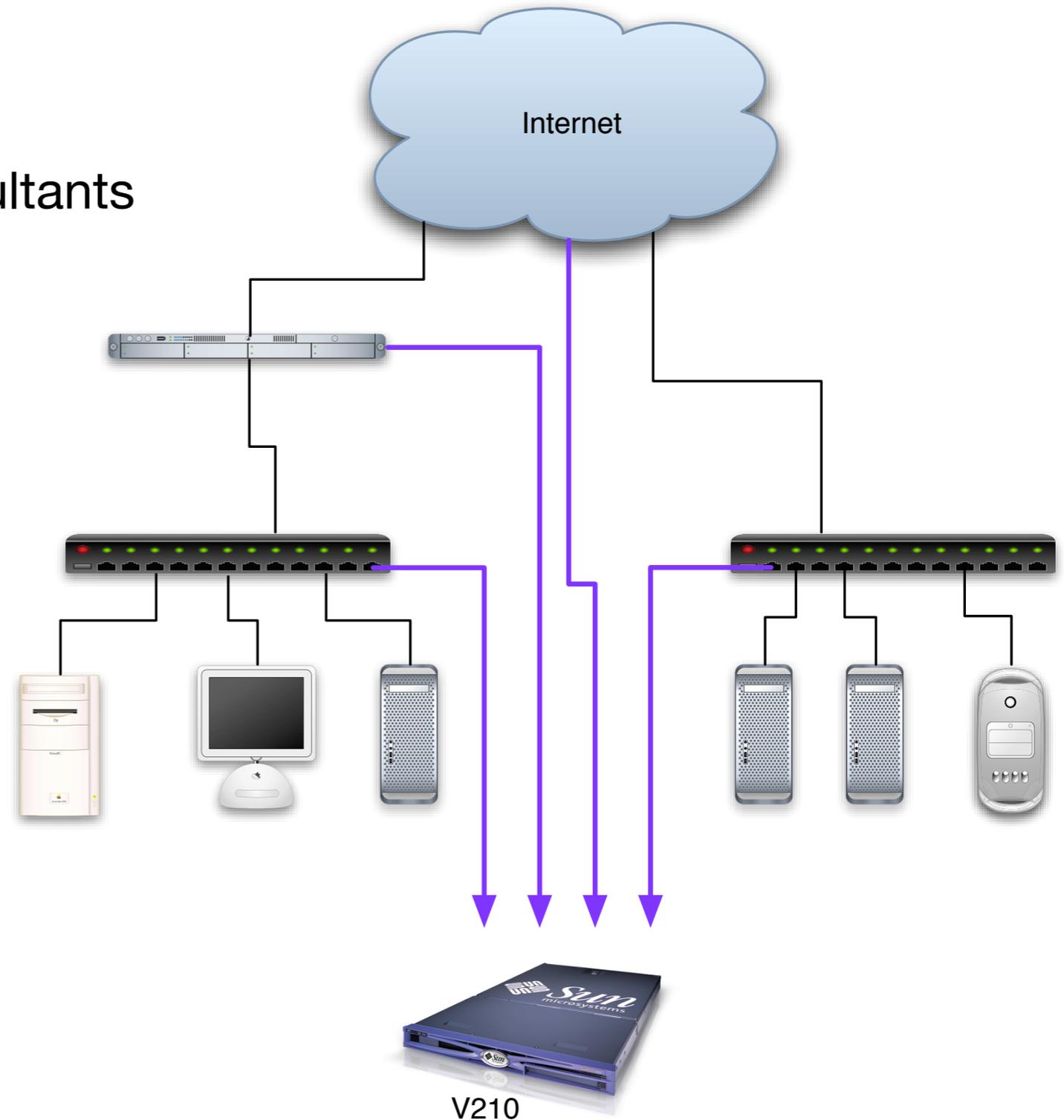
Flow-based systems: “blind” to data

Advantages:

- More economical
- Finds rogue servers and consultants
- More privacy-sensitive

Can't discover:

- Missing encryption
- Inappropriate encryption
- Protocols on wrong ports
- Leaking specific documents



Flow-based vendors

Arbor Networks

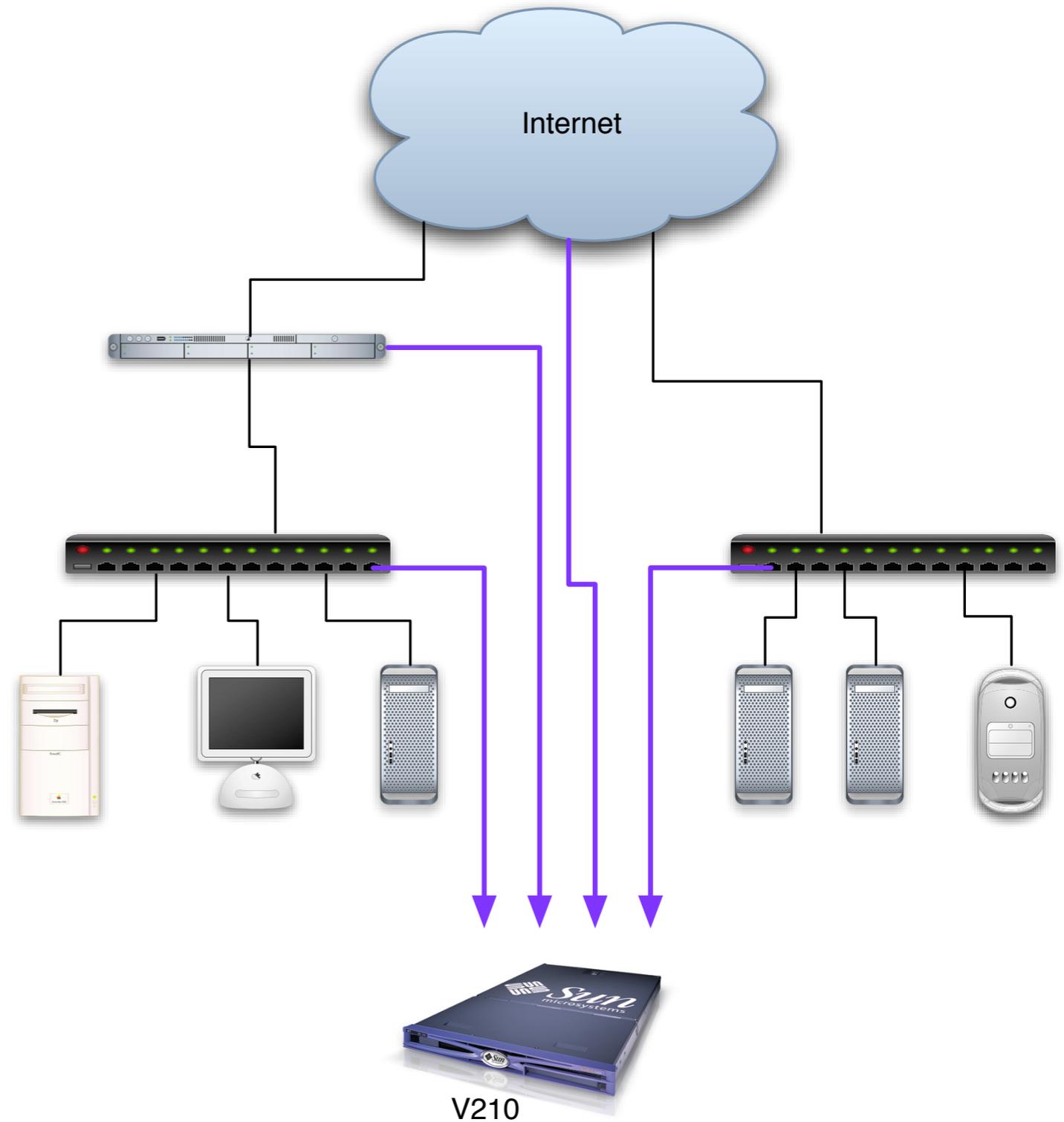
GraniteEdge Networks

Lanscope

Mazu Networks

Q1 Labs

...and many more



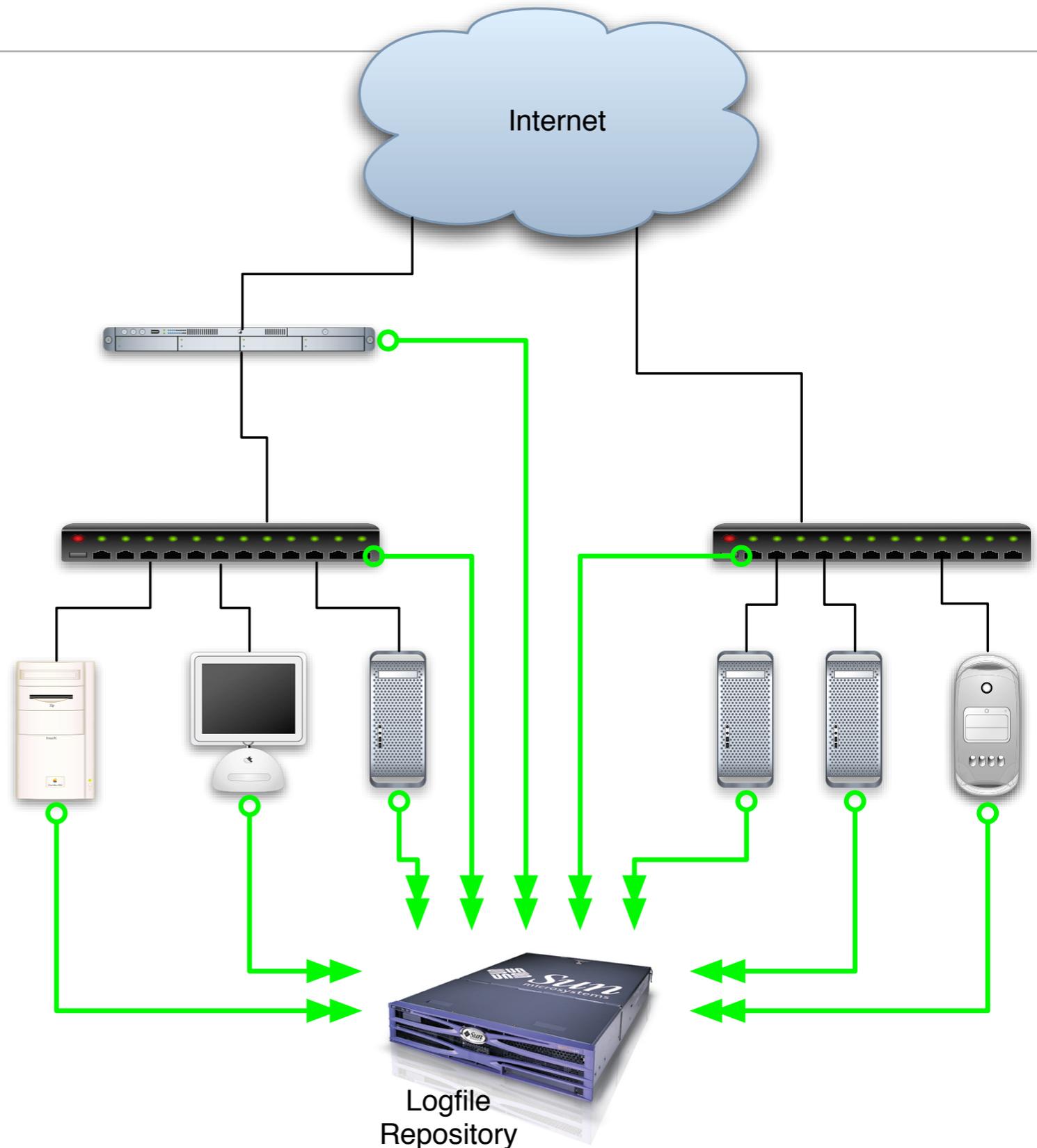
Log files: options

Open Source Options:

- syslog

Commercial Options:

- LogLogic
- Netforensics
- Q1 Labs
- Many other options...



[REDACTED]

[REDACTED]

The Department's attorney workforce is **more diverse than the U.S. legal workforce**: 38% female, compared to 30% in the U.S. legal labor pool, and 15% minority, compared to 12% in the labor pool. The Department's attorney workforce is about **as diverse as the federal government legal workforce**, whose attorneys are 38% female and 16% minority.

Hiring is serving to make the Department even more diverse: hires in 2001 were 40% female and 21% minority.

[REDACTED] Honors Program hires in 2001 were 63% female, compared to 45% of the law school graduating class, and 30% minority, compared to 21% of the class of 2001.

Minorities [REDACTED] They comprise only 7% of (career) SES attorneys and 11% of supervisory Assistant U.S. Attorneys. Women constitute 31% of SESs and 37% of supervisory AUSAs. Among GS-15 attorneys in the Litigating Divisions, minorities comprise 11% of non-supervisors and 6% of supervisors, and women comprise 37% of non-supervisors and 33% of supervisors.

[REDACTED] In 2001, the attrition rate was 49% higher among minorities than whites. There was no difference in recent attrition between men and women.

[REDACTED] For example, the average minority GS attorney is currently 0.4 steps lower than the average white, and the average woman is 0.3 steps lower than the average man, controlling for seniority, grade, and component.

Based on these findings, we recommend that the Department take the following actions:

[REDACTED]

Uses for Document Forensics

Which computer generated this document?

Who edited this document?

What was changed? When?

Is this document “authentic?”

Approaches for Data and Document Analysis:

Look for hidden data:

- Deleted information; previous versions
- GIDs embedded in Microsoft Word document

Look for characteristic data:

- Indicates authorship
- Indicates program used to create document.

Look for inconsistent data:

- Indicates possible tampering.

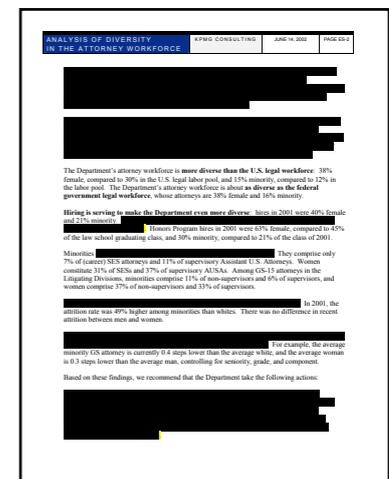
Privacy and Security violations result when improperly sanitized documents are released.

Adobe PDF files:

- The New York Times published a PDF file containing the names of Iranians who helped with the 1953 coup. (2000) (<http://cryptome.org/cia-iran.htm>)
- US DoJ published a PDF file “diversity report” with embarrassing redacted information. (2003) (<http://www.thememoryhole.org/feds/doj-attorney-diversity.htm>)
- Multinational Force-Iraq report (2005)

Microsoft Word Files:

- SCO Word file revealed its anti-Linux legal strategy. (2004)
- Intelligence report by Blair Government was found to be plagiarized from a postgraduate student at the Monterey Institute of International Studies based on transaction log (2003)
<http://www.computerbytesman.com/privacy/blair.htm>



Why is data left in documents?

1. Confusion between “covering data” and removing it.
2. Failure to implement “complete delete.”
3. Information that is written but never read.

Most Acrobat leakage is a result of Microsoft Word.

[REDACTED]

[REDACTED]

The Department's attorney workforce is **more diverse than the U.S. legal workforce**: 38% female, compared to 30% in the U.S. legal labor pool, and 15% minority, compared to 12% in the labor pool. The Department's attorney workforce is about **as diverse as the federal government legal workforce**, whose attorneys are 38% female and 16% minority.

Hiring is serving to make the Department even more diverse: hires in 2001 were 40% female and 21% minority. [REDACTED] Honors Program hires in 2001 were 63% female, compared to 45% of the law school graduating class, and 30% minority, compared to 21% of the class of 2001.

Minorities [REDACTED] They comprise only 7% of (career) SES attorneys and 11% of supervisory Assistant U.S. Attorneys. Women constitute 31% of SESs and 37% of supervisory AUSAs. Among GS-15 attorneys in the Litigating Divisions, minorities comprise 11% of non-supervisors and 6% of supervisors, and women comprise 37% of non-supervisors and 33% of supervisors.

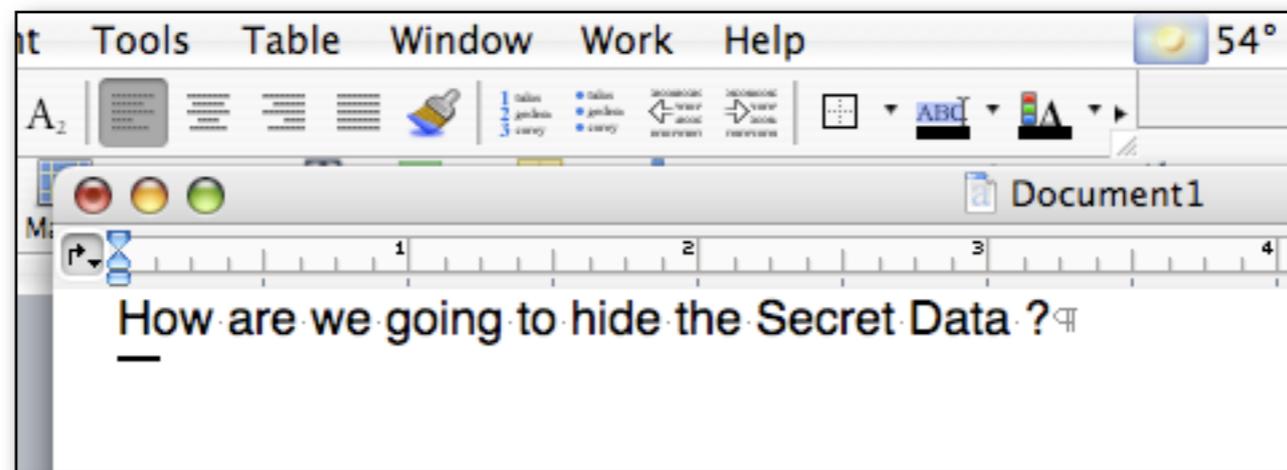
[REDACTED] In 2001, the attrition rate was 49% higher among minorities than whites. There was no difference in recent attrition between men and women.

[REDACTED] For example, the average minority GS attorney is currently 0.4 steps lower than the average white, and the average woman is 0.3 steps lower than the average man, controlling for seniority, grade, and component.

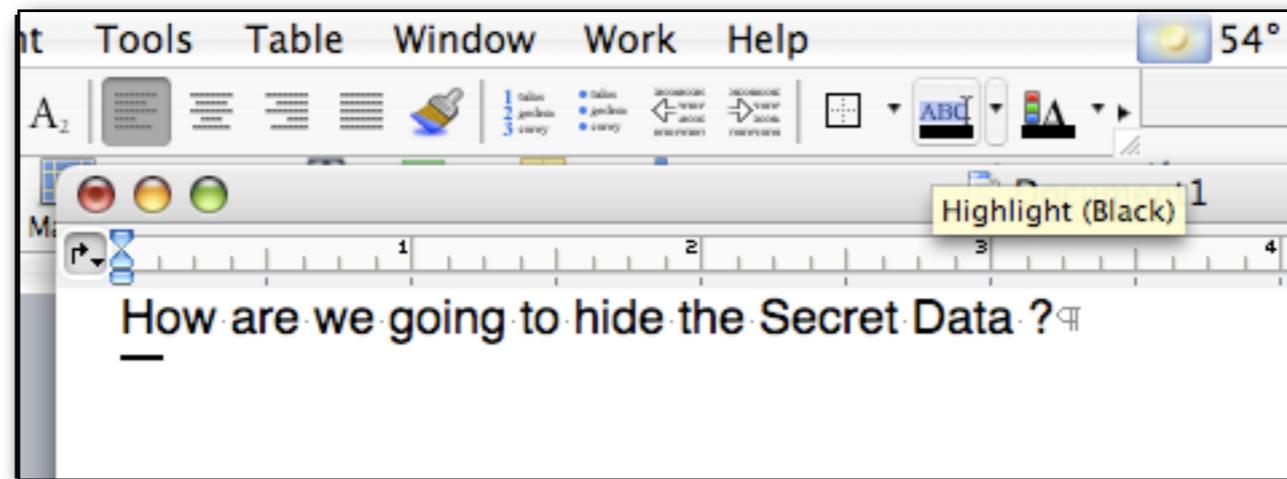
Based on these findings, we recommend that the Department take the following actions:

[REDACTED]

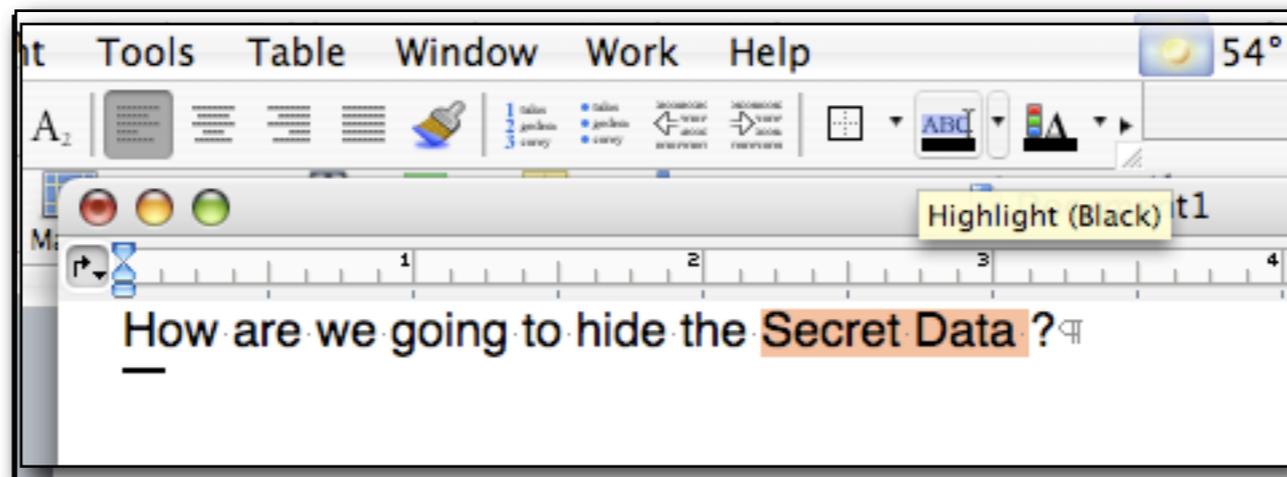
Microsoft Word encourages people to use the highlight feature to eradicate data.



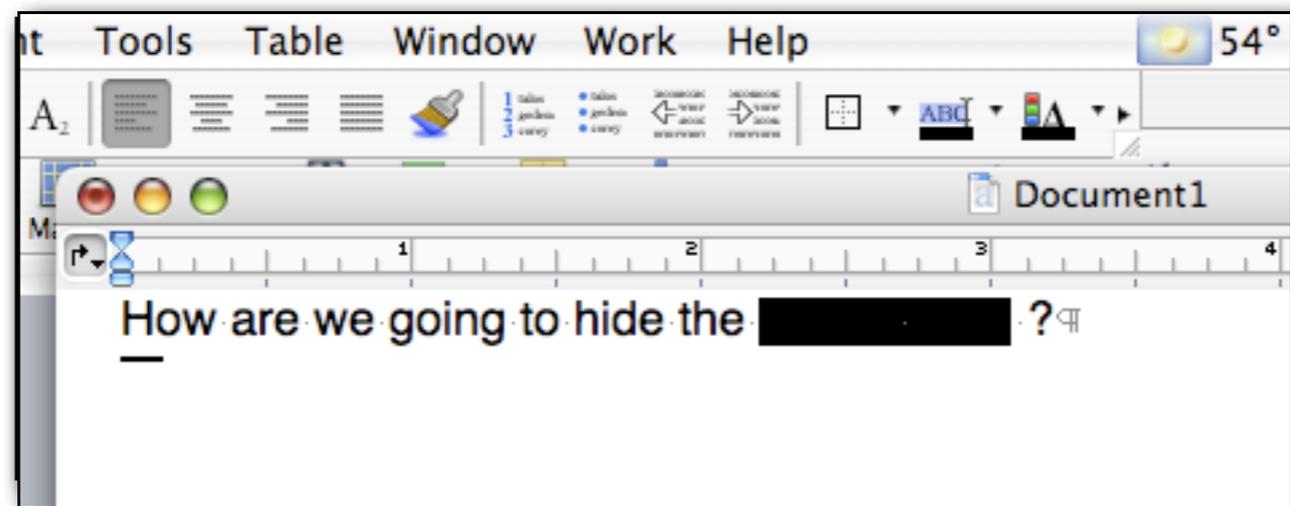
Microsoft Word encourages people to use the highlight feature to eradicate data.



Microsoft Word encourages people to use the highlight feature to eradicate data.



Microsoft Word encourages people to use the highlight feature to eradicate data.



When Microsoft Word generates the PDF file,
“Secret Data” is covered with the black box



Tools for recovering hidden data in Acrobat files:

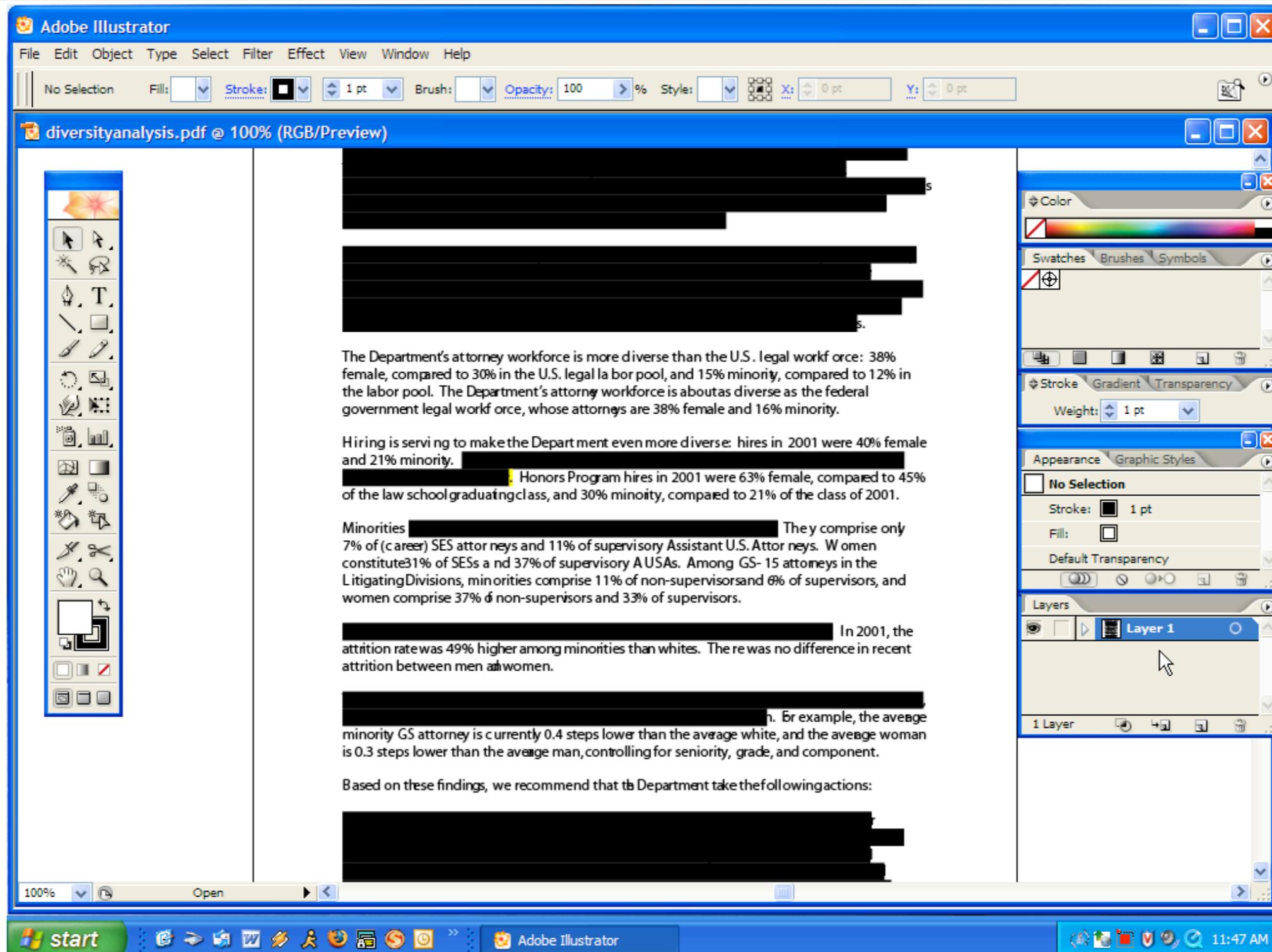
Adobe Illustrator

- Move the boxes
- Turn the boxes yellow

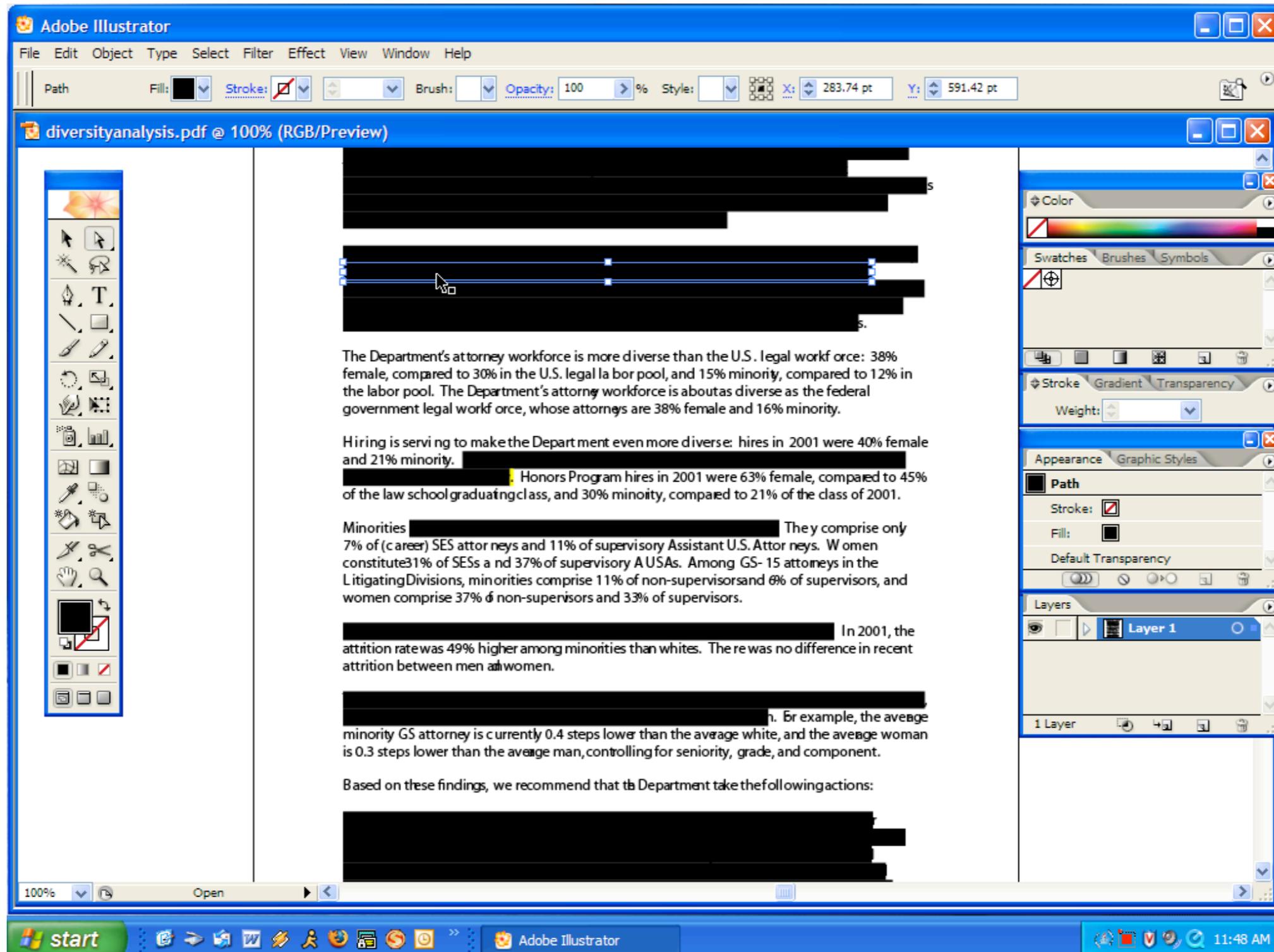
Adobe Acrobat Reader

- Select and copy the text

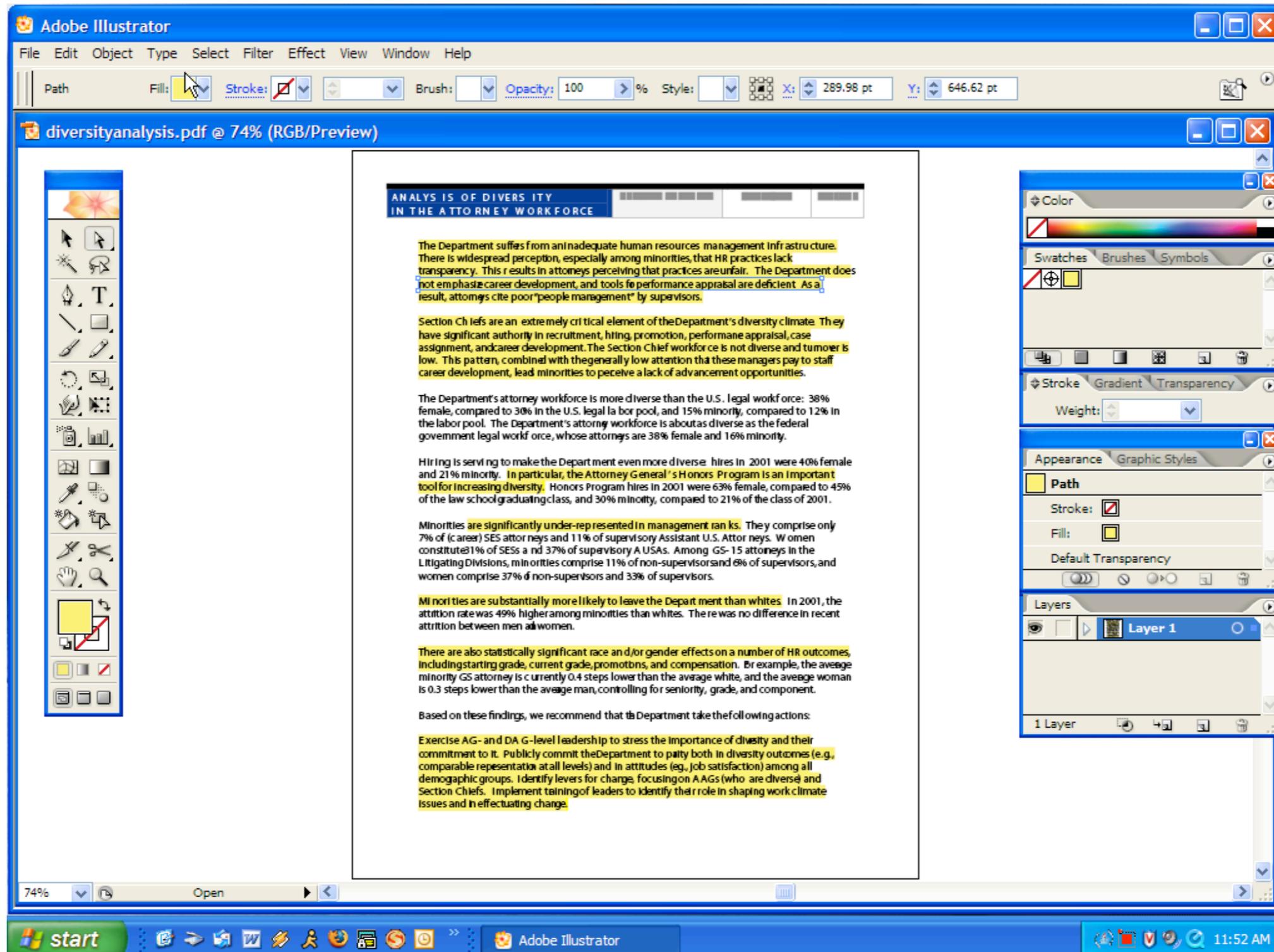
Adobe's Illustrator can read and edit PDF files.



Select each “block box.”



Change the color of the box to yellow.



Behold the “redacted” data.

The Department suffers from an inadequate human resources management infrastructure. There is widespread perception, especially among minorities, that HR practices lack transparency. This results in attorneys perceiving that practices are unfair. The Department does not emphasize career development, and tools for performance appraisal are deficient. As a result, attorneys cite poor “people management” by supervisors.

Section Chiefs are an extremely critical element of the Department’s diversity climate. They have significant authority in recruitment, hiring, promotion, performance appraisal, case assignment, and career development. The Section Chief workforce is not diverse and turnover is low. This pattern, combined with the generally low attention that these managers pay to staff career development, lead minorities to perceive a lack of advancement opportunities.

The Department’s attorney workforce is more diverse than the U.S. legal workforce: 38% female, compared to 30% in the U.S. legal labor pool, and 15% minority, compared to 12% in the labor pool. The Department’s attorney workforce is about as diverse as the federal government legal workforce, whose attorneys are 38% female and 16% minority.

Hiring is serving to make the Department even more diverse: hires in 2001 were 40% female and 21% minority. In particular, the Attorney General’s Honors Program is an important tool for increasing diversity. Honors Program hires in 2001 were 63% female, compared to 45% of the law school graduating class, and 30% minority, compared to 21% of the class of 2001.

Minorities are significantly under-represented in management ranks. They comprise only 7% of (career) SES attorneys and 11% of supervisory Assistant U.S. Attorneys. Women constitute 31% of SESs and 37% of supervisory AUSAs. Among GS-15 attorneys in the Litigating Divisions, minorities comprise 11% of non-supervisors and 6% of supervisors, and women comprise 37% of non-supervisors and 33% of supervisors.

Minorities are substantially more likely to leave the Department than whites. In 2001, the attrition rate was 49% higher among minorities than whites. There was no difference in recent attrition between men and women.

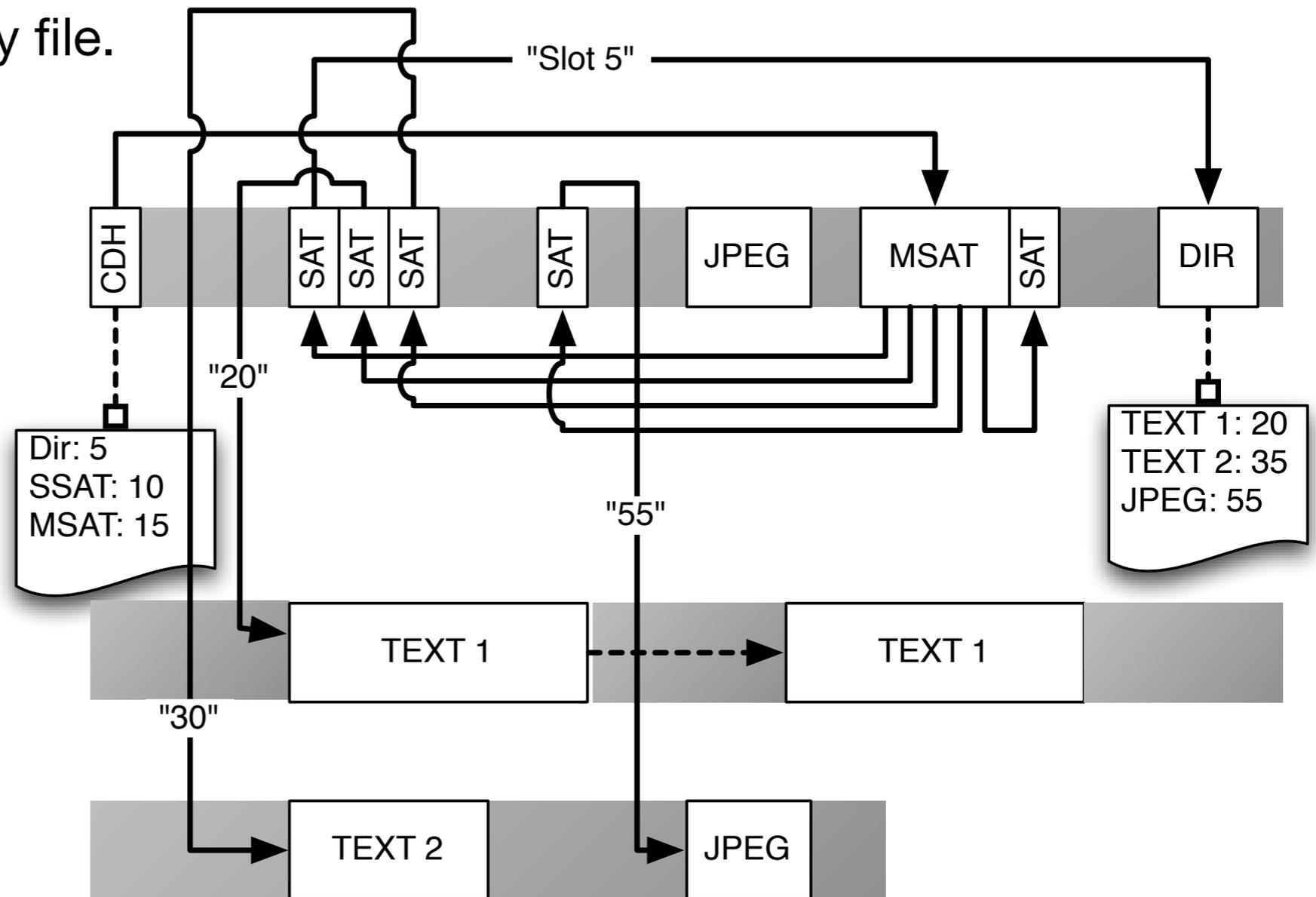
There are also statistically significant race and/or gender effects on a number of HR outcomes, including starting grade, current grade, promotions, and compensation. For example, the average minority GS attorney is currently 0.4 steps lower than the average white, and the average woman is 0.3 steps lower than the average man, controlling for seniority, grade, and component.

Based on these findings, we recommend that the Department take the following actions:

Exercise AG- and DAG-level leadership to stress the importance of diversity and their commitment to it. Publicly commit the Department to parity both in diversity outcomes (e.g., comparable representation at all levels) and in attitudes (e.g., job satisfaction) among all demographic groups. Identify levers for change, focusing on AAGs (who are diverse) and Section Chiefs. Implement training of leaders to identify their role in shaping work climate issues and in effectuating change.

Data can be left in a Word document in unallocated sectors.

Microsoft Word implements a "file system" inside every file.



Tools for recovering hidden Word data:

Unix strings(1) command reveals:

- Deleted text
- Names and/or usernames of author and editors
- Paths where document was saved
- GUID of system on which it was saved

Note: Text may be UTF16 (remove NULLs or use more intelligent processing)

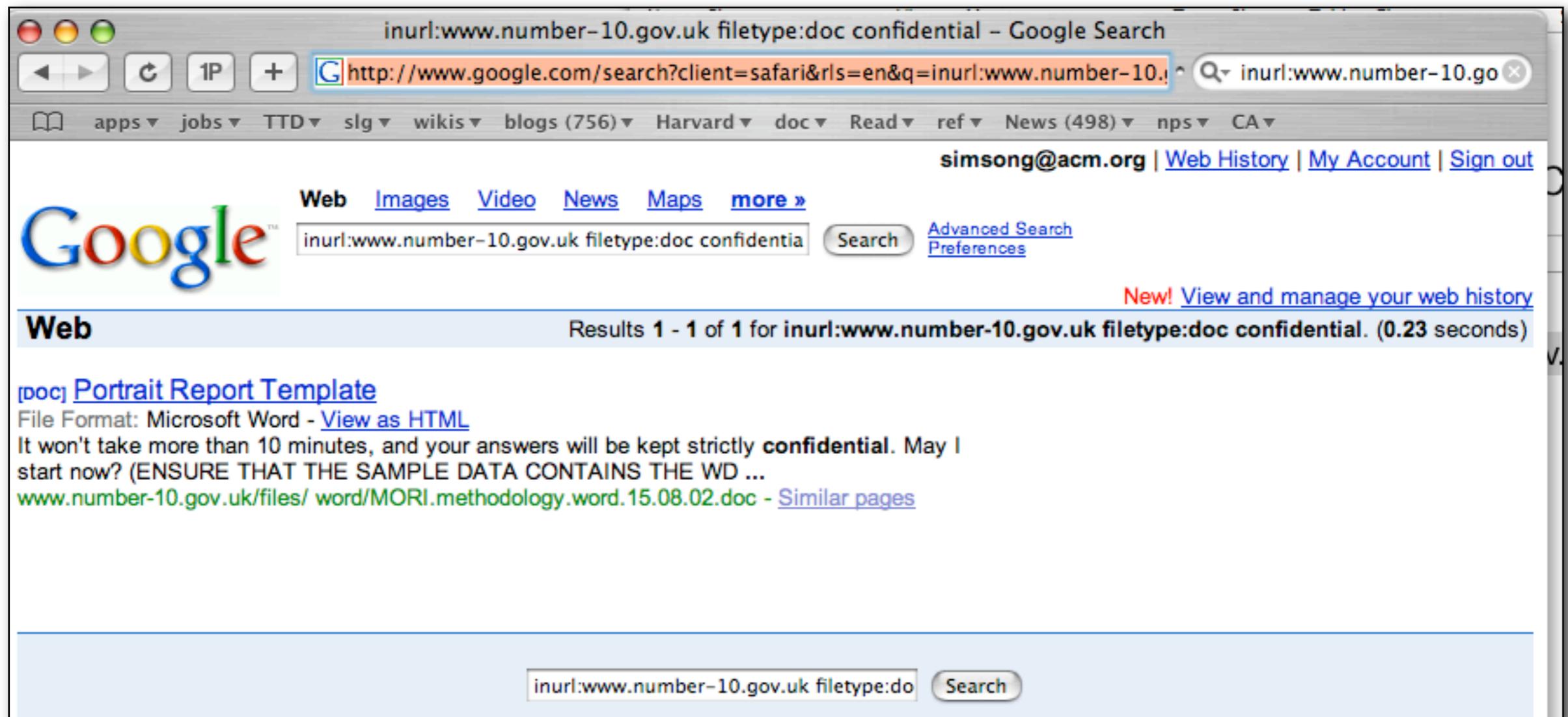
Other tools:

- Antiword (<http://www.winfield.demon.nl/>)
- catdoc
- wvText
- MITRE's Heuristic Office File Format Analysis toolkit (HOFFA)

Tools for finding Microsoft Word files

Use Google!

- `inurl:www.number-10.gov.uk filetype:doc confidential`



Case study of inconsistent data: State of Utah vs. Carl Payne

```
lp:NP:6445:.....  
smtp:*NP:6445:.....  
uucp:NP:6445:.....  
nuucp:NP:6445:.....  
listen:*LK*:.....  
nobody:NP:6445:.....  
noaccess:NP:6445:.....  
setup:ANImj3G8/T3m2:6445:.....  
ftp:NP:6445:.....  
carl:*1rwuFse0eS/S6:9807:.....  
majo:NP:.....
```

State of Utah vs. Carl Payne

State's Claims:

- Victim ISP suffered devastating attack on November 6th, 1996.
 - All files erased
 - All router configurations cleared.
- Carl Payne, one of the company's founders, had a falling out with the company and was terminated on October 30th, 1996.
- Payne had the necessary knowledge to carry out the attack.
- Payne created a "back door" on his last week of employment.
- Payne's accounts were used for the attack.

State of Utah vs. Carl Payne

State's Evidence:

- 140 pages of printouts made by a local expert on the day of the attack.
- Testimony of the expert.
- Testimony of the Fibernet employees

Payne's Defense:

- "I didn't do it."
- All of Payne's account passwords had been changed when he was terminated.
- Alibi defense: was having breakfast with a friend when attack took place.

/etc/shadow

(printed November 6, 1996)

```
root:0rtdD.YmG4mNA:9818::::::
daemon:NP:6445::::::
bin:NP:6445::::::
sys:NP:6445::::::
adm:NP:6445::::::
lp:NP:6445::::::
smtp:*NP:6445::::::
uucp:NP:6445::::::
nuucp:NP:6445::::::
listen:*LK*::::::
nobody:NP:6445::::::
noaccess:NP:6445::::::
setup:ANImj3G8/T3m2:6445::::::
ftp:NP:6445::::::
carl:*1rwuFse0eS/S6:9807::::::
majo:NP:::::::
news:::::::
dbowling:*n.56DqWPfcZ6w:9807::::::
hart:YqEuyT.mD8buc:::::::
usenet:*Lq.mMF7KaEdd.:9800::::::
```

Solaris /etc/shadow:

```
setup:ANImj3G8/T3m2:64455::::::
```

Field 1: Username

Field 2: Encrypted Password

Field 3: Password Aging

- Number of days since January 1, 1970

Source: Solaris Documentation

Decoding “6645”

August 25, 1987

```
mysql> select from_days(to_days('1970-01-01')+6445);
```

```
+-----+
| from_days(to_days('1970-01-01')+6445) |
+-----+
| 1987-08-25                             |
+-----+
```

```
1 row in set (0.00 sec)
```

```
mysql>
```

/etc/shadow

(Printed November 6, 1996 by prosecution expert witness)

```
root:0rtdD.YmG4mNA:9818::::::
daemon:NP:6445::::::
bin:NP:6445::::::
sys:NP:6445::::::
adm:NP:6445::::::
lp:NP:6445::::::
smtp:*NP:6445::::::
uucp:NP:6445::::::
nuucp:NP:6445::::::
listen:*LK*::::::
nobody:NP:6445::::::
noaccess:NP:6445::::::
setup:ANImj3G8/T3m2:6445::::::
ftp:NP:6445::::::
carl:*1rwuFse0eS/S6:9807::::::
majo:NP:::::::
news:::::::
dbowling:*n.56DqWPfcZ6w:9807::::::
hart:YqEuyT.mD8buc:::::::
usenet:*Lq.mMF7KaEdd.:9800::::::
```

9818 = November 18, 1996

6445 = August 25, 1987

9807 = November 7, 1996

9800 = October 31, 1996

Lessons of Utah vs. Payne

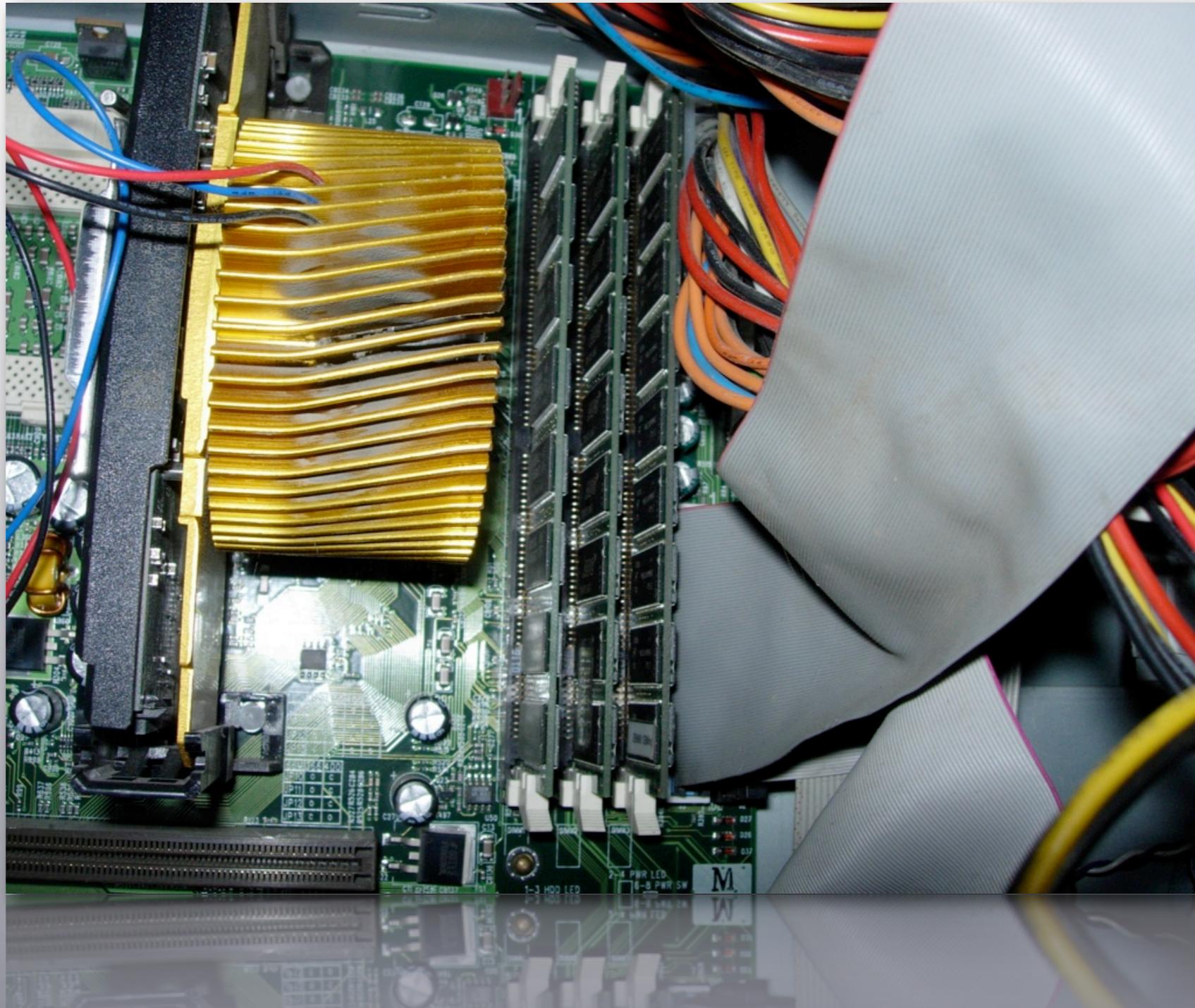
Not all “Evidence” is equal (Chain-of-custody is vital)

Evidence may not prove what you think it proves

Computer evidence lends itself to forgery

Most data isn't tampered...

- ... but most data isn't used for evidence.
- If data *is* going to be used for evidence, there is an incentive to tamper with it.

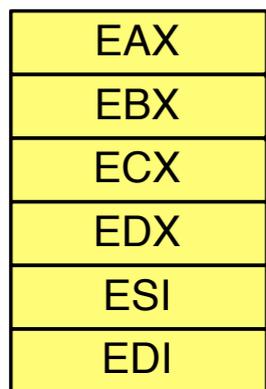


Memory Forensics

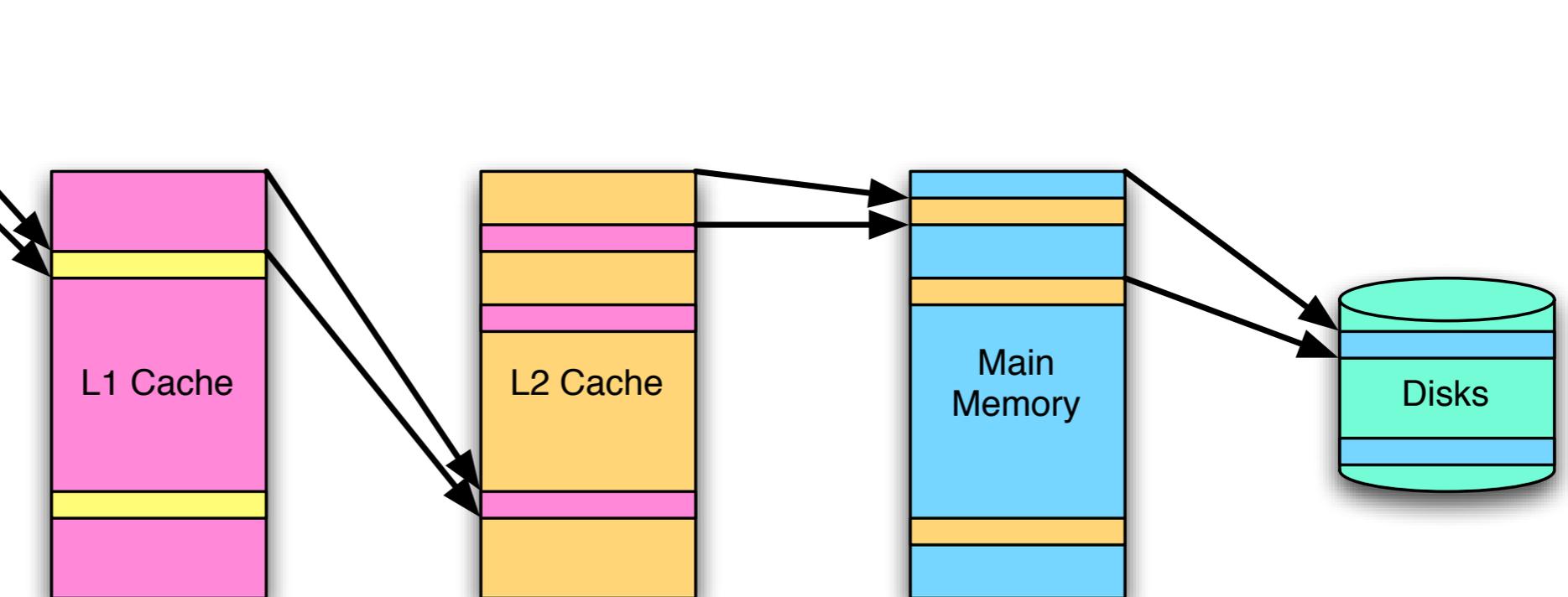
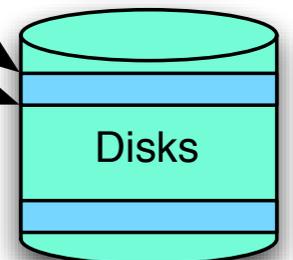
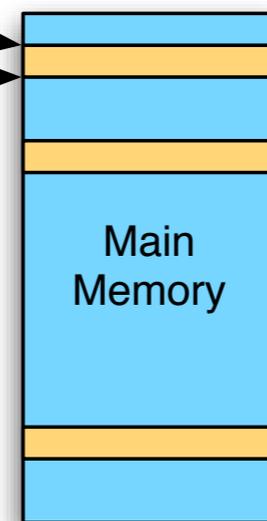
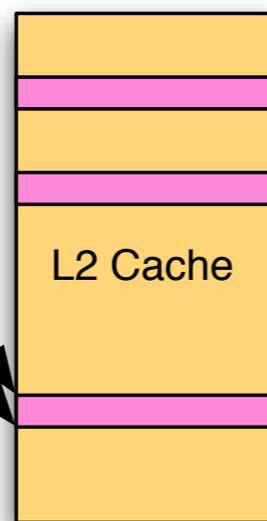
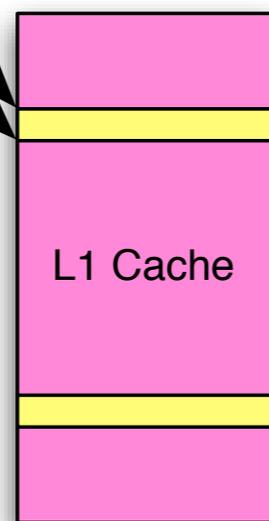
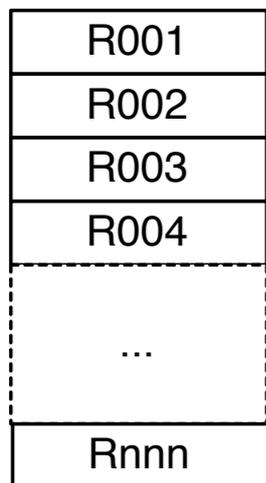
What was *really* happening on the subject's computer?

Computer systems arrange memory in a hierarchy.

Architectural Registers



Active Register File



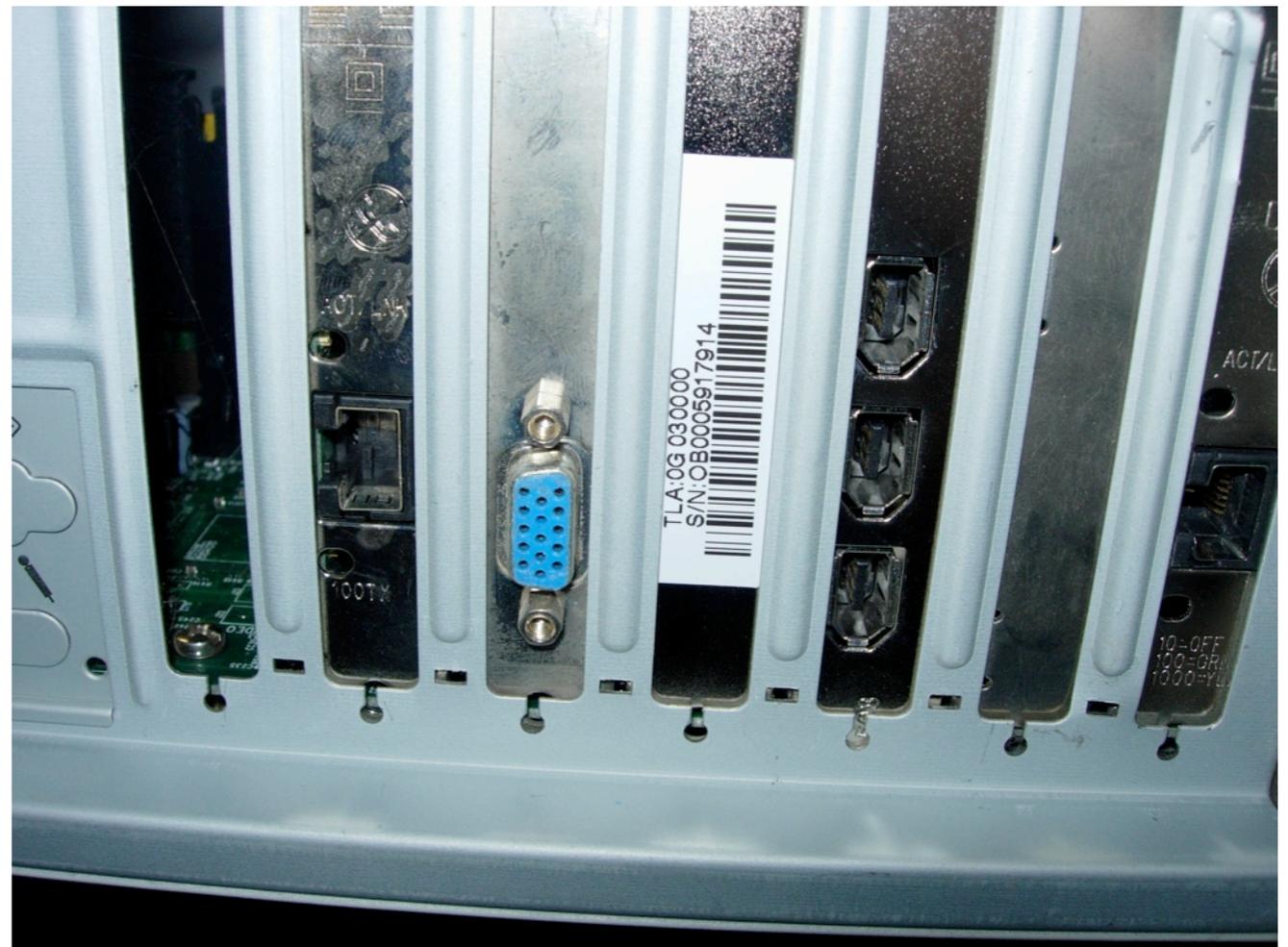
There are many ways to acquire the memory.

Swap space on live or dead systems

- PAGEFILE.SYS
- /private/var/vm/swapfile
- Swap Partitions

Live Memory:

- /dev/mem
- /proc/kcore
- \\.\PhysicalMemory
- \\.\DebugMemory
- Device Drivers
- Hardware memory imagers
- *Firewire*
- *Suspend/Resume*



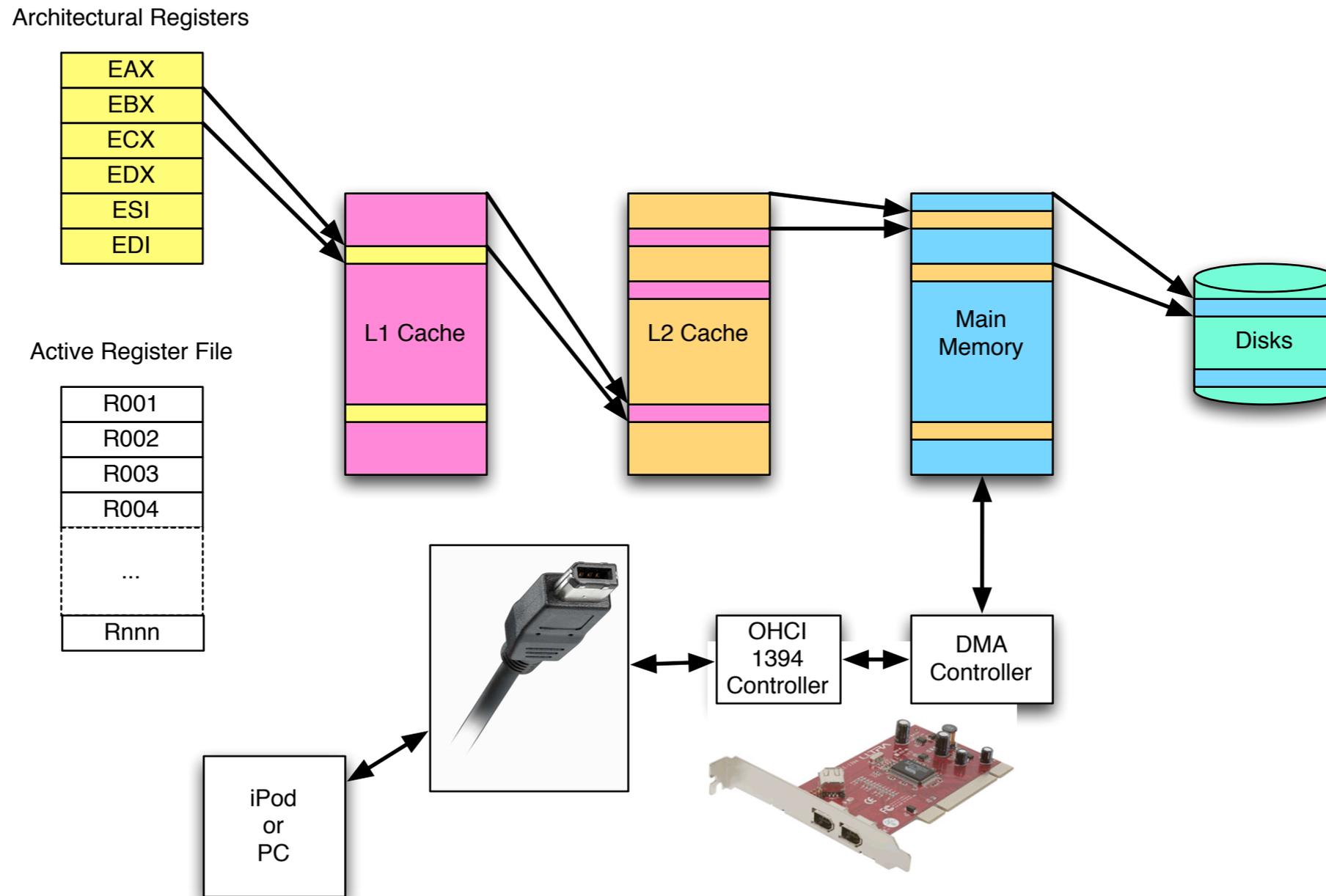
Potential problems with acquiring physical memory

Memory changes fast; it won't be consistent.

Software methods can be blocked by attacker.

Physical memory needs to be mapped to virtual memory for most kinds of analysis.

It's pretty easy to attack a system with an iPod

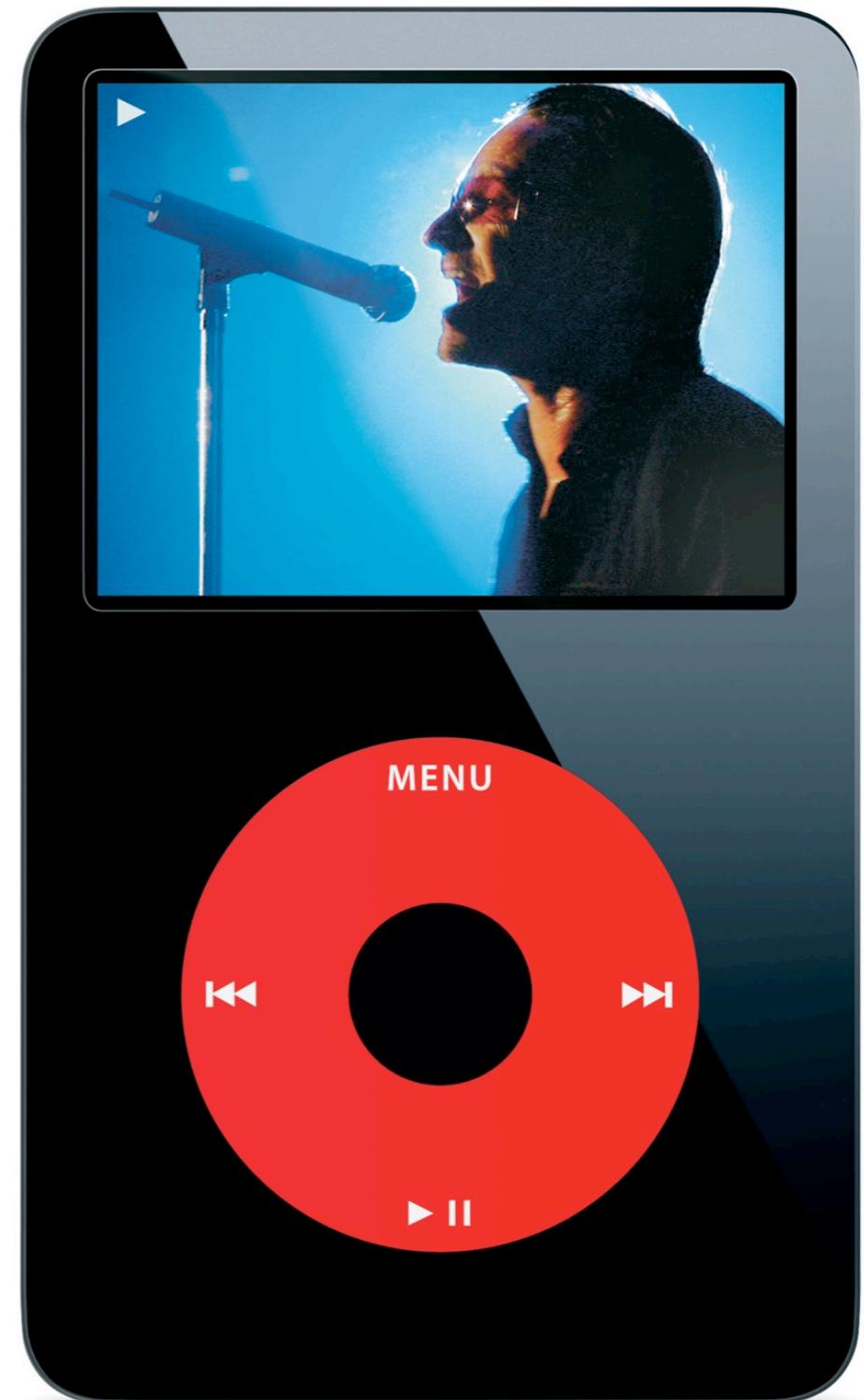


DMA bypasses the operating system and the CPU.

Many different kinds of information can be retrieved from a computer's memory.

Reading:

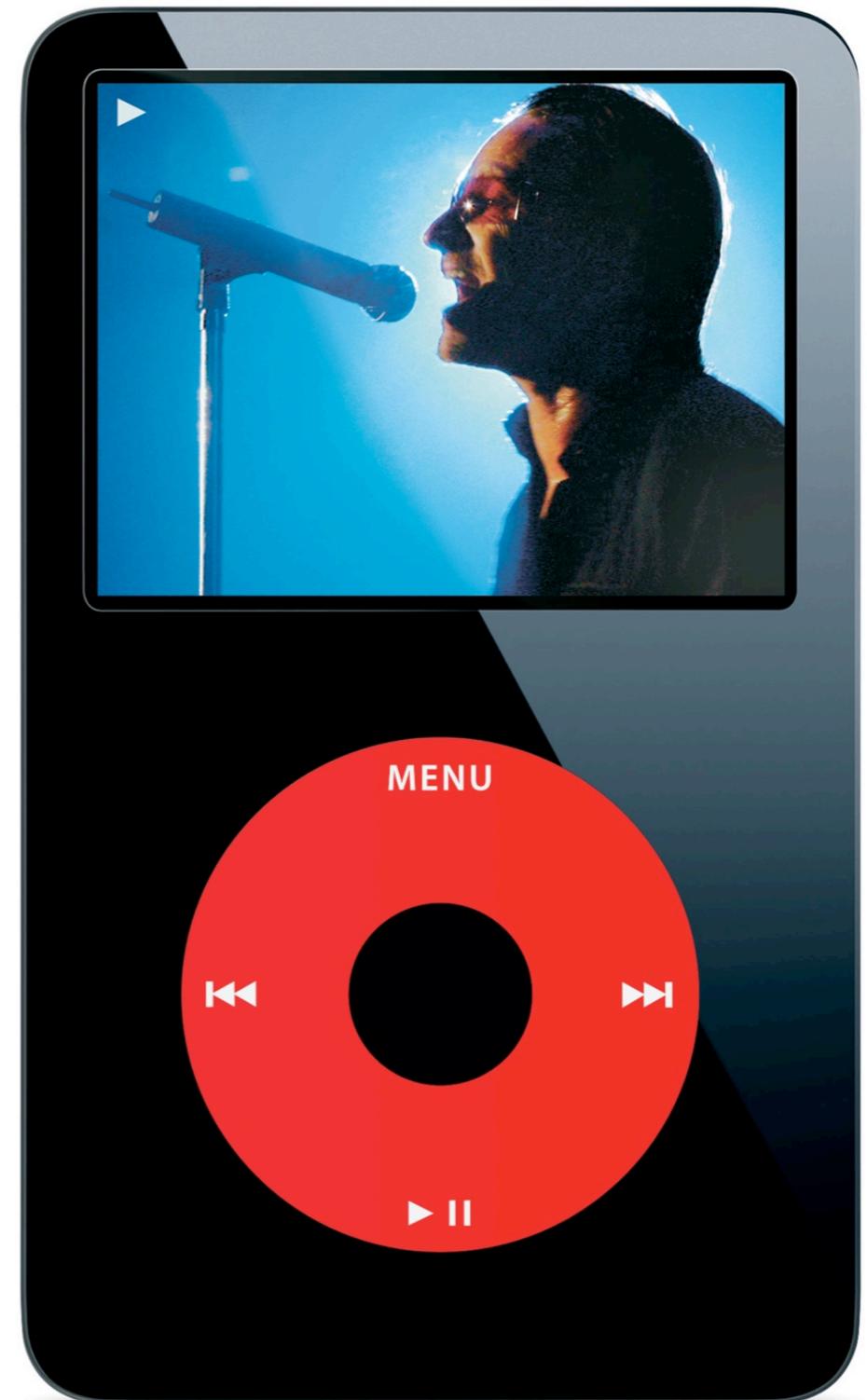
- Contents of the screen
- Cryptographic Keys
- Passwords (BIOS & programs)
- Current Running Programs
- Remnants of previously run programs
- Open TCP/UDP ports
- Cached data
- Hidden data



Systems can be taken over by writing memory

Patch programs on the fly

Change security levels



Memory Analysis Techniques

Look for ASCII and UNICODE strings.

- strings(1), grep

File carving

- foremost, scalpel

Identify and interpret kernel or program data structures

Convert Windows memory image to Microsoft crashdump format, then analyze with standard debugging tools:

- http://computer.forensikblog.de/en/2006/03/dmp_file_structure.html

KnTTools (Windows), by George M. Garner, Jr.

KNTDD - Acquires memory

- Acquisition to removable drive or network
- Cryptographic integrity checks, auditing
- Conversion to Microsoft crash dump format
- Remote deployment as a service

KnTList - Lists Kernel Structures

- Reconstructs virtual address space
- Drives, Device Objects, System Tables
- Threads, access tokens, handle table, objects, etc.
- Outputs as text and XML

<http://forensic.seccure.net/>

<http://users.erols.com/gmgarner/KnTTools/>

WMFT - Windows Memory Forensic Toolkit

Enumerates processes, modules, libraries

Finds hidden data (rootkits)

Detailed information:

- Access tokens
- Handles
- Processes
- Modules

<http://forensic.seccure.net/>

Idetect (Linux)

Displays detailed information for each process

Enumerates all process-related structures

Can work on memory image or live system

- <http://forensic.seccure.net/tools/idetect.tar.gz>
- http://forensic.seccure.net/pdf/mburdach_digital_forensics_of_physical_memory.pdf

Lots more information about memory forensics, including 53-page presentation:

- <http://forensic.seccure.net>





Cell Phone and PDA Forensics

Who did you call?
Where have you been?

PDAs and Cellphones:

Difficult times for computer forensics

Powerful computers

- 100–300Mhz processors
- 16MB – 2GB of RAM (or more)
- Cellular, Bluetooth, WiFi & IR networking
- Cameras

Little standardization:

- PalmOS, Windows Mobile, Symbian, RIM, Linux, & other OS
- Many different cables

Other challenges:

- Some systems lose memory w/o power
- Smart phones have 2 processors & memories
- Removable Media

As a result, different phones typically require different tools.



Cell phones are part of a system

Public Telephone Switched Network

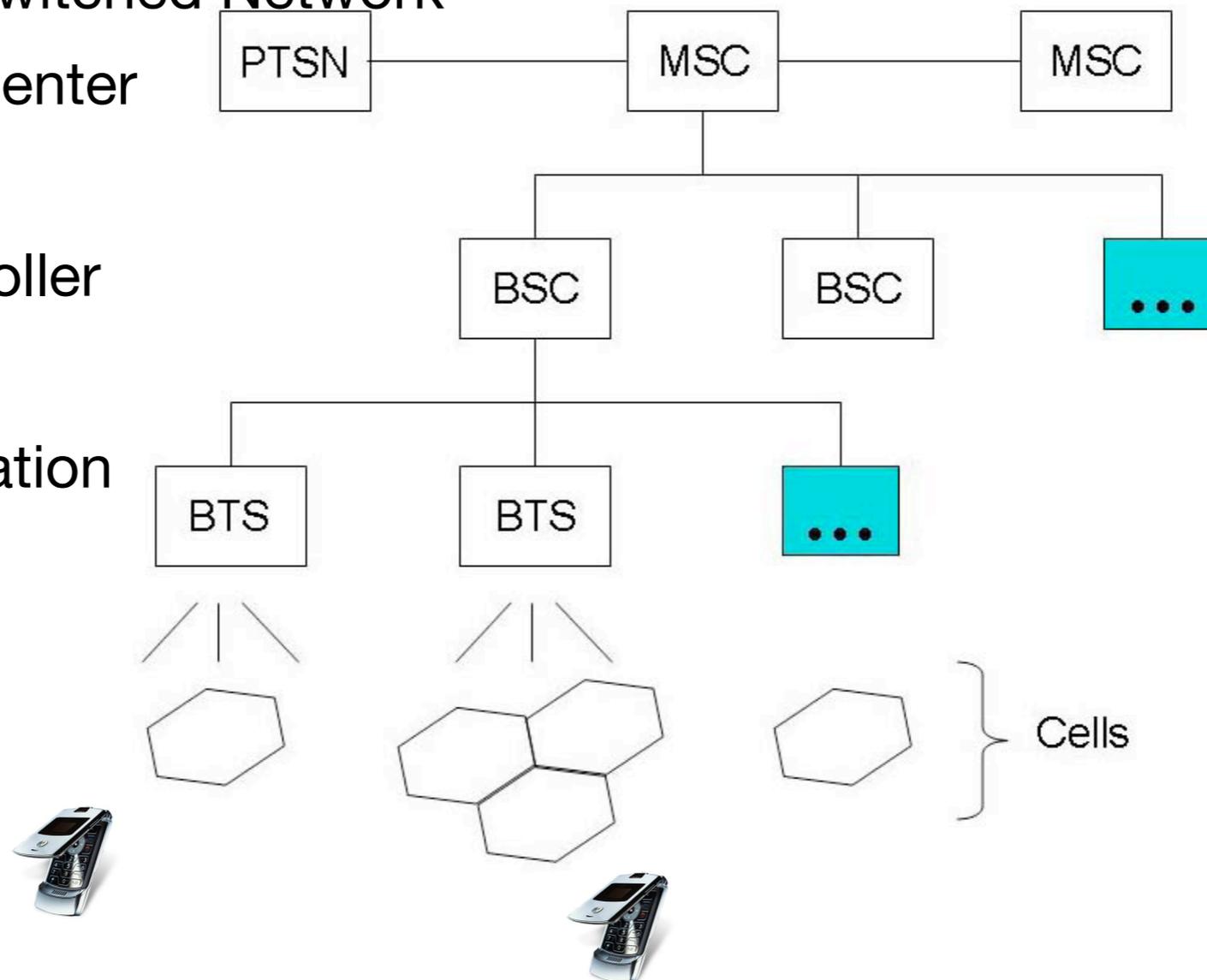
Mobile Switching Center

Base Station Controller

Base Tranceiver Station

Cell sites

Cell phones



Software of a typical cell phone:

	Basic	Advanced	Smart
OS	Proprietary	Proprietary	Linux, Windows Mobile, Palm OS, Symbian, RIM
PIM	Simple Phonebook	Phonebook and Calendar	Reminder List, Enhanced Phonebook, Calendar
Applications	None	MP3 Player	MP3 Player, Office Document Viewing
Messaging	Text Messaging	Text with Images	Text, Images, Movies
Chat	None	SMS Chat	SMS & Instant Messaging
Email	None	Via Network Operator's Service Gateway	Via POP or IMAP
Web	None	Via WAP Gateway	Direct HTTP
Wireless	IrDA	IrDA, Bluetooth	IrDA, Bluetooth, Wi-Fi

Source: NIST Guidelines on Cell Phone Forensics, p. 9

Identity Module Characteristics

GSM:

- Subscriber Identity Modules (SIMs) 16K-128K
- Mobile Equipment (ME) identifier
- IMEI - International Mobile Equipment Identifier (*#06#)
- Some information is stored in the phone, some information is stored in the SIM.

CDMA:

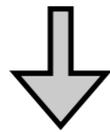
- Electronic Serial Number (ESN)
- MSID
- All information stored in phone



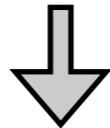
Source: NISTTIR 7250
Wikipedia

Cell phone forensic tools: Broad Categories

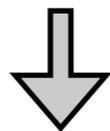
Tools that use the cell phone's own keyboard & display



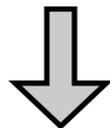
Tools that download information through the cell phone's standard ports



Tools that access cell phone through programmer/proprietary ports



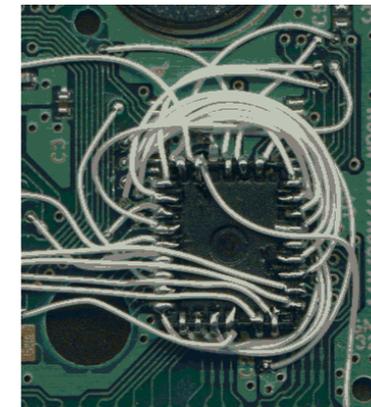
SIM readers



Direct access to flash through circuit board



Project-a-Phone



Accessories

“StrongHold Box” prevents phone from calling home.



“Device Seizure Toolbox” has lots of different cables.



<http://www.paraben-forensics.com/>

Acquisition

Identify the device: make, model, service provider.

- Necessary to select the appropriate tool.
- <http://www.phonescoop.com/phones/finder.php>
- <http://www.gsmarena.com/search.php3>
- <http://mobile.softpedia.com/phoneFinder>

Also note:

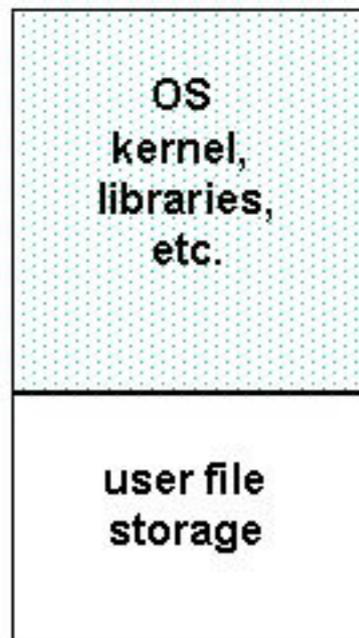
- Device Interface, labels, serial numbers, etc.
- Synchronization software on associated computer
- Time displayed by phone

Memory Considerations

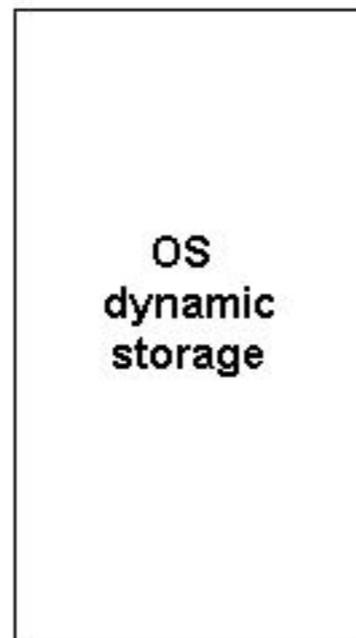
Mobile phones have multiple memory systems.

SIM file system

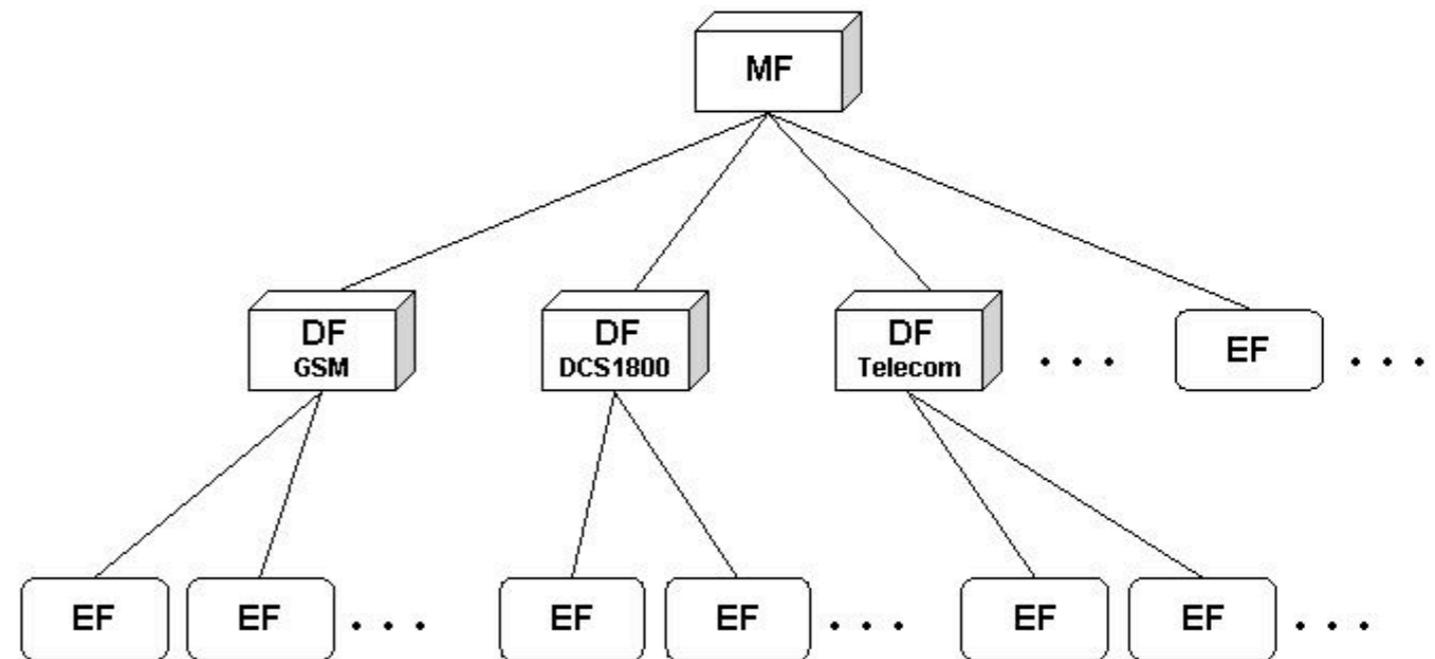
Non-Volatile Memory



Volatile Memory



Telephone Service
OS



Unobstructed Devices

Typically done with a forensically sound tool, if possible.

Separately acquire the phone memory & SIM card.

Usually requires phone to be turned on — which can cause problems

Unobstructed Devices

Typically done with a forensically sound tool, if possible.

Separately acquire the phone memory & SIM card.

Usually requires phone to be turned on

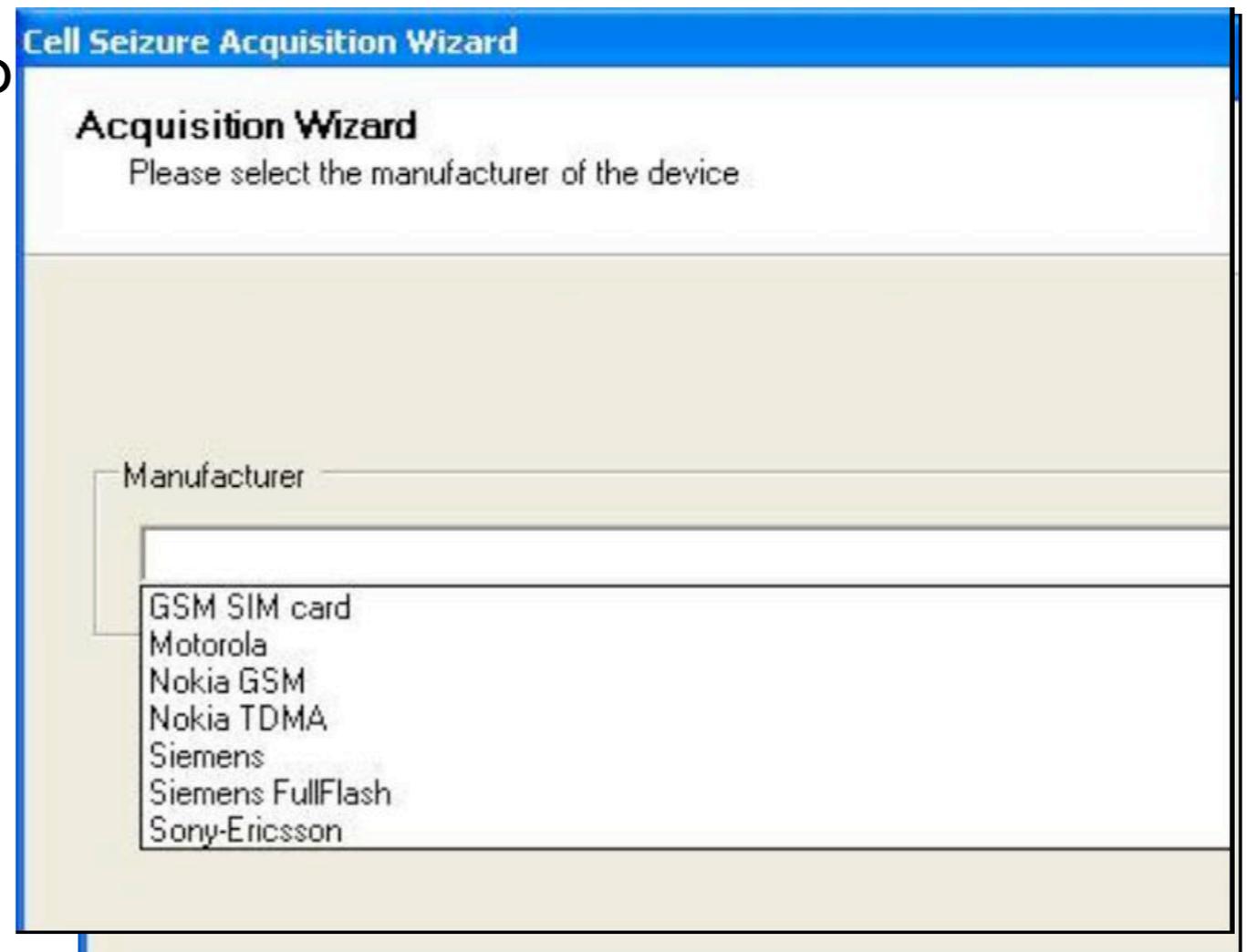


Unobstructed Devices

Typically done with a forensically sound tool, if possible.

Separately acquire the phone memory & SIM card.

Usually requires phone to be turned o

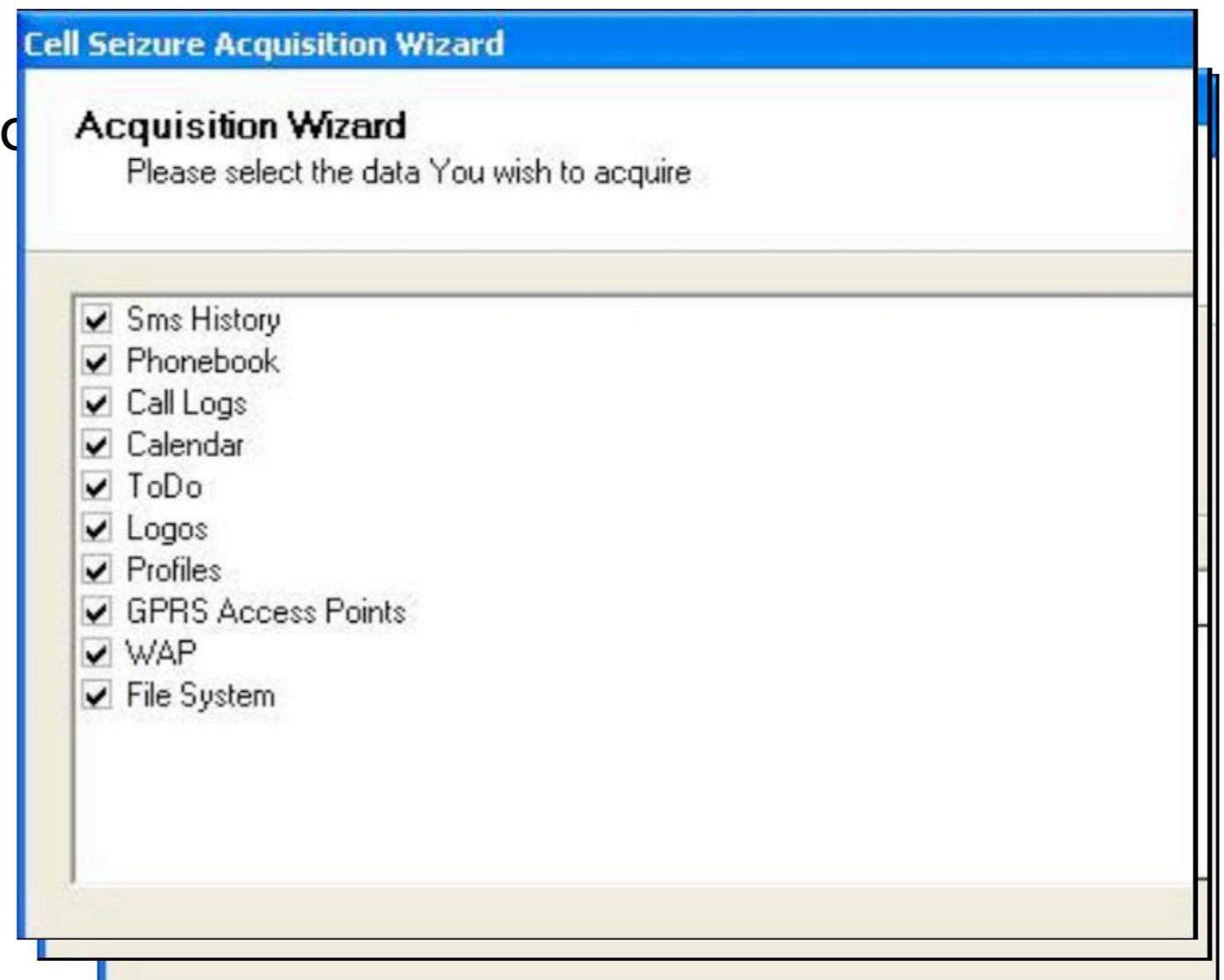


Unobstructed Devices

Typically done with a forensically sound tool, if possible.

Separately acquire the phone memory & SIM card.

Usually requires phone to be turned on

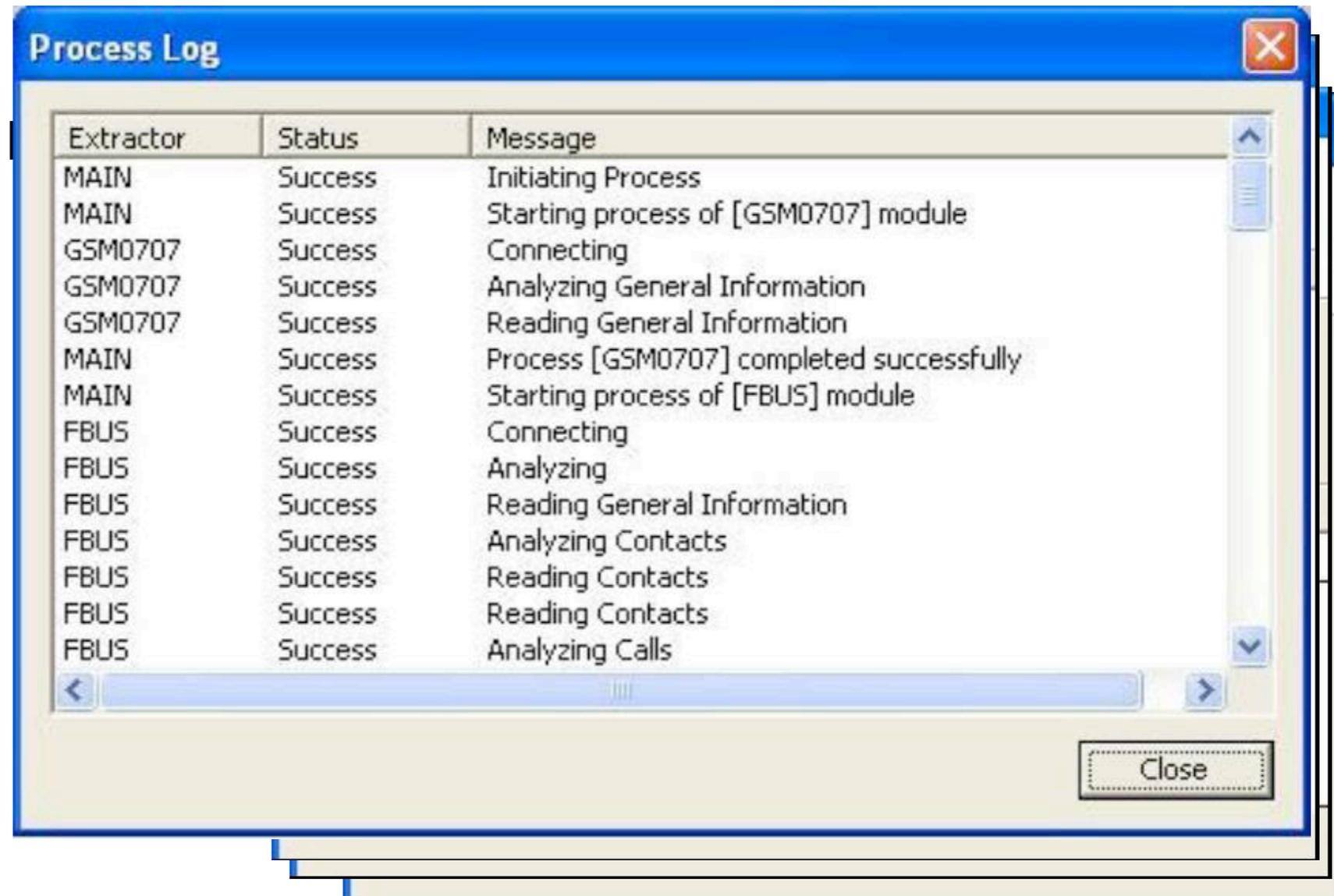


Unobstructed Devices

Typically done with a forensically sound tool, if possible.

Separately acquire the phone memory & SIM card.

Usually requires phone to be



Obstructed Devices

Password-protected phones or SIM cards.

“Content encryption capabilities are currently not offered in the retail cell phone market.”

Options:

- Backdoor from manufacturer
- Professionals who know how to attack the hardware
- Search Internet for developer information or hacker exploits.

Other options:

- Ask the suspect for the password, PIN, or other information.
- Review seized material.
- Guess (try 1234, etc.)
- Ask service provider for PUK code (GSM)

Obstructed Devices — Examples

PalmOS version 4.0 or earlier: password easily reversed after memory downloaded during sync.

Netherlands Forensic Institute has general-purpose tool for examining memory chips.

Nokia handsets have master password that can be calculated from equipment identifier.

iPAQ 3900 and other models support “parrot bootloader

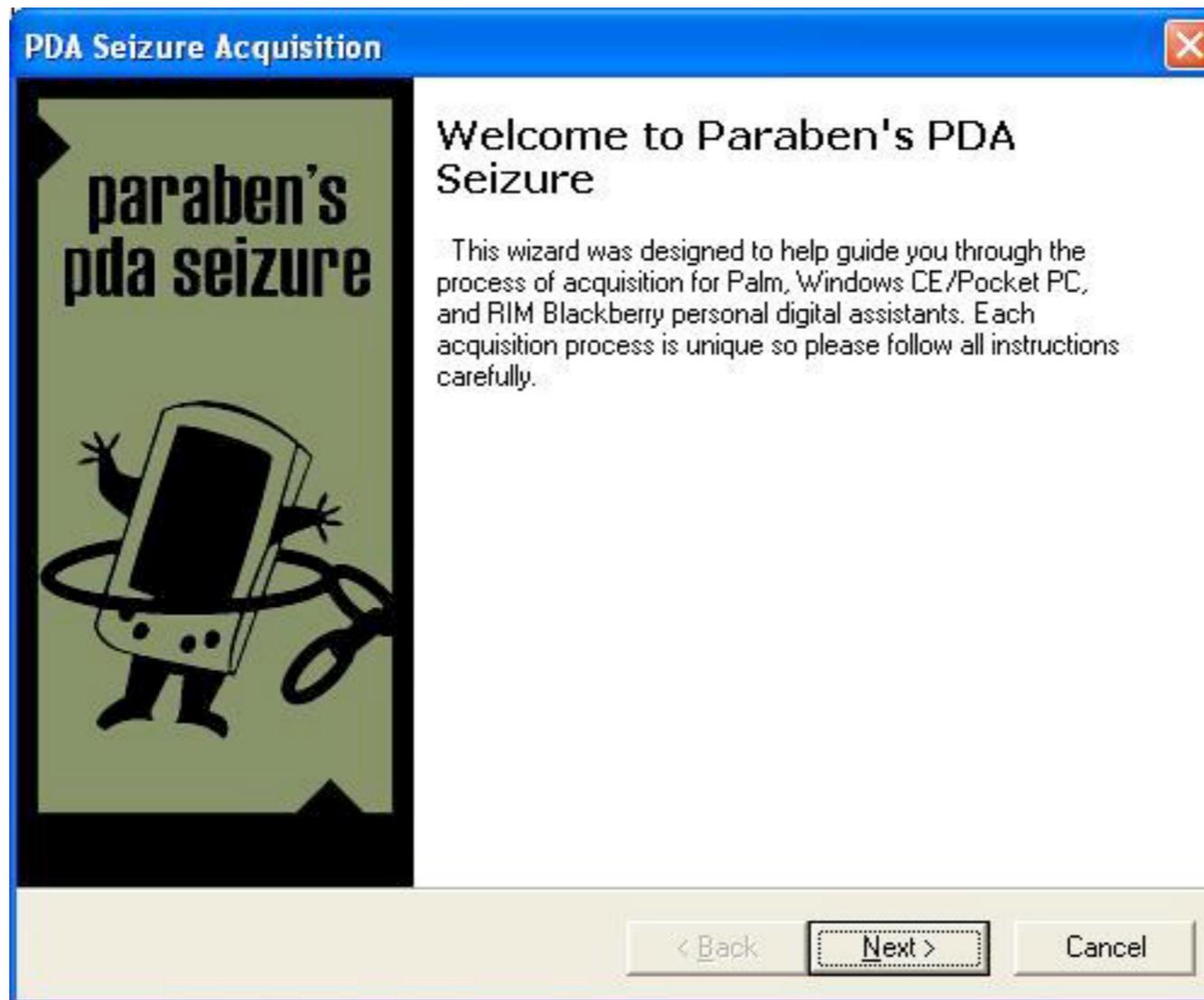
Create a substitute (U)SIM card to take over the phone.

- Forensic SIM Toolkit
- GSM .XRY SIM Id Cloner
- TULP 2G SIMIC

Examination and Analysis

- Subscriber & equipment identifiers
- Date/time
- language and other settings
- Phonebook
- Appointment Calendar
- Text Messages
- Dialed, incoming, & missed call log
- Electronic mail
- Photos
- Audio and video records
- Multi-media messages
- Instant messages
- Web browsing records
- Electronic Documents
- Location information

Paraben's PDA Seizure



Paraben's PDA Seizure

C:\Documents and Settings\Administrator\Desktop\cell acquisition data\Samsung_i700\Samsung_010504_1.PDA - PDA Seizure

File Edit Tools View Help

Files Search Graphics Bookmarks

File Path	File Name	Type	Create Date	Modify Date	Attri...	Size	Status	Location	MD5 Hash
{My Documents}	pic0001.jpg	.jpg	2005/01/05 12:41:52	2005/01/05 12:41:52	CA	27,495	Acquired	RAM	AA2B8B265DAAE3FF1D7DD36ACFA09283
{My Documents}	PIC0000.TMB	.TMB	2005/01/05 12:41:02	2005/01/05 12:41:02	CA	9,270	Acquired	RAM	03726217B9886CF17C6DD0C1A0709B10
{My Documents}	pic0000.jpg	.jpg	2005/01/05 12:41:02	2005/01/05 12:41:02	CA	41,231	Acquired	RAM	FFA24DFEFC6EA6D28478175C134D036
{My Documents}\My Pictures}	Sunset.jpg	.jpg	2005/01/05 12:46:48	2005/01/05 12:46:48	CA	71,189	Acquired	RAM	1BC5B77F3E50B7FBE12C792EE438DA45
{My Documents}\My Pictures}	french.mp3	.mp3	2005/01/05 12:46:31	2005/01/05 12:46:31	CA	7,523	Acquired	RAM	A2B4FD7568F735463D11D9BAD0A29938
{My Documents}\My Pictures}	chare.wav	.wav	2005/01/05 12:46:28	2005/01/05 12:46:28	CA	39,694	Acquired	RAM	FCB34DE0D5E433A2B64A45A8A265BFD3
{My Documents}\My Pictures}	winter.bmp	.bmp	2005/01/05 12:46:23	2005/01/05 12:46:23	CA	353,478	Acquired	RAM	3632A33D141A8759065AD3588E40CA25
{My Documents}\My Pictures}	Beer.png	.png	2005/01/05 12:46:18	2005/01/05 12:46:18	CA	2,548	Acquired	RAM	1B5BA7972C0F642A5E59D8A38DECF6A5
{My Documents}\Templates}	Vehicle Mileage Log.pxt	.pxt	2003/03/21 08:20:56	2003/03/21 08:20:56	CHRA	7,498	Acquired	RAM	9C91BBE9B134B471A1330DB64FA87134
{My Documents}\Templates}	To Do.psw	.psw	2003/03/21 08:20:56	2003/03/21 08:20:56	CHRA	2,616	Acquired	RAM	0F7982DEE180764A7ACB88757DA1001B
{My Documents}\Templates}	Phone Memo.psw	.psw	2003/03/21 08:20:56	2003/03/21 08:20:56	CHRA	2,008	Acquired	RAM	9443F21C4AC49604D371BDCD848E0F3
{My Documents}\Templates}	Memo.psw	.psw	2003/03/21 08:20:56	2003/03/21 08:20:56	CHRA	2,112	Acquired	RAM	523694AF6762CF19DB802B8E2436DFE0
{My Documents}\Templates}	Meeting Notes.psw	.psw	2003/03/21 08:20:55	2003/03/21 08:20:55	CHRA	1,908	Acquired	RAM	40FB8E424E340886885482228E45AB97
{My Documents}\Templates}	Blank Document.psw	.psw	2003/03/21 08:20:55	2003/03/21 08:20:55	CHRA	0	Acquired	RAM	
{My Documents}\Templates}	To Do.pwi	.pwi	2003/03/21 08:20:55	2003/03/21 08:20:55	CHRA	3,096	Acquired	RAM	B25EAC50156BC12E6FAD5ABCEACBFA29
{My Documents}\Templates}	Phone Memo.pwi	.pwi	2003/03/21 08:20:55	2003/03/21 08:20:55	CHRA	2,008	Acquired	RAM	7F2CCAB0FE75072F7AB89DCD1D7136B3
{My Documents}\Templates}	Memo.pwi	.pwi	2003/03/21 08:20:55	2003/03/21 08:20:55	CHRA	2,112	Acquired	RAM	CAC4C826FBA6F47AD9D088941343D5D4
{My Documents}\Templates}	Meeting Notes.pwi	.pwi	2003/03/21 08:20:55	2003/03/21 08:20:55	CHRA	1,592	Acquired	RAM	B876D7DE671DE6DCCBAC8D5726DCDE82
{My Documents}\Templates}	Blank Note.pwi	.pwi	2003/03/21 08:20:55	2003/03/21 08:20:55	CHRA	0	Acquired	RAM	
{Windows}	CESeizure.dll	.dll	2005/01/05 12:51:04	2005/01/05 12:51:04	CA	4,608	Acquired	RAM	148E9FEDDEB1F90CD42DAA78DDA0E58E
{Windows}	System.mky	.mky	2003/03/21 16:24:04	2003/03/21 16:24:04	CHSA	52	Acquired	RAM	D02937A4B0BB164D2AD71C0676B5A7E6
{Windows}	MsgQueueMapFileMicroso		2005/01/05 12:45:54	2005/01/05 12:45:54	CA	268,292	Acquired	RAM	1ED7E3BF7DFF04456B7002C946F37E0E
{Windows}	MsgQueueDataFileMicrosc		2005/01/05 12:45:54	2005/01/05 12:45:54	CA	2,850,820	Acquired	RAM	987F1B368E0A33EDA33EDACEF80D783EC4834
{Windows}\Messaging}	0000192d1000001f.mpb	.mpb	2005/01/05 12:44:01	2005/01/05 12:44:01	CA	2	Acquired	RAM	C4103F122D27677C9DB144CAE1394A66
{Windows}\Messaging}	0000192d81030102.mpb	.mpb	2005/01/05 12:43:05	2005/01/05 12:43:05	CA	0	Acquired	RAM	
{Windows}\Messaging}	010017b81000001f.mpb	.mpb	2003/03/23 16:14:11	2003/03/23 16:14:11	CA	2	Acquired	RAM	C4103F122D27677C9DB144CAE1394A66
{Windows}\Messaging}\Attachme	192d-1931.att	.att	2005/01/05 12:43:04	2005/01/05 12:43:04	CA	13,320	Acquired	RAM	933F8BC6F80311C84B6EE11527975580
{Windows}\Messaging}\Attachme	192d-1931.att	.att	2003/03/21 16:21:17	2003/03/21 16:21:17	CHSA	133	Acquired	RAM	501550F1D0F001E7A0741E00A0E5E5A0

861 Files

NUM

Paraben's PDA Seizure

C:\Documents and Settings\Administrator\Desktop\cell acquisition data\Samsung_i700\Samsung_122004_2.PDA - PDA Seizure

File Edit Tools View Help

Files Search Graphics Bookmarks

homer simpson Search

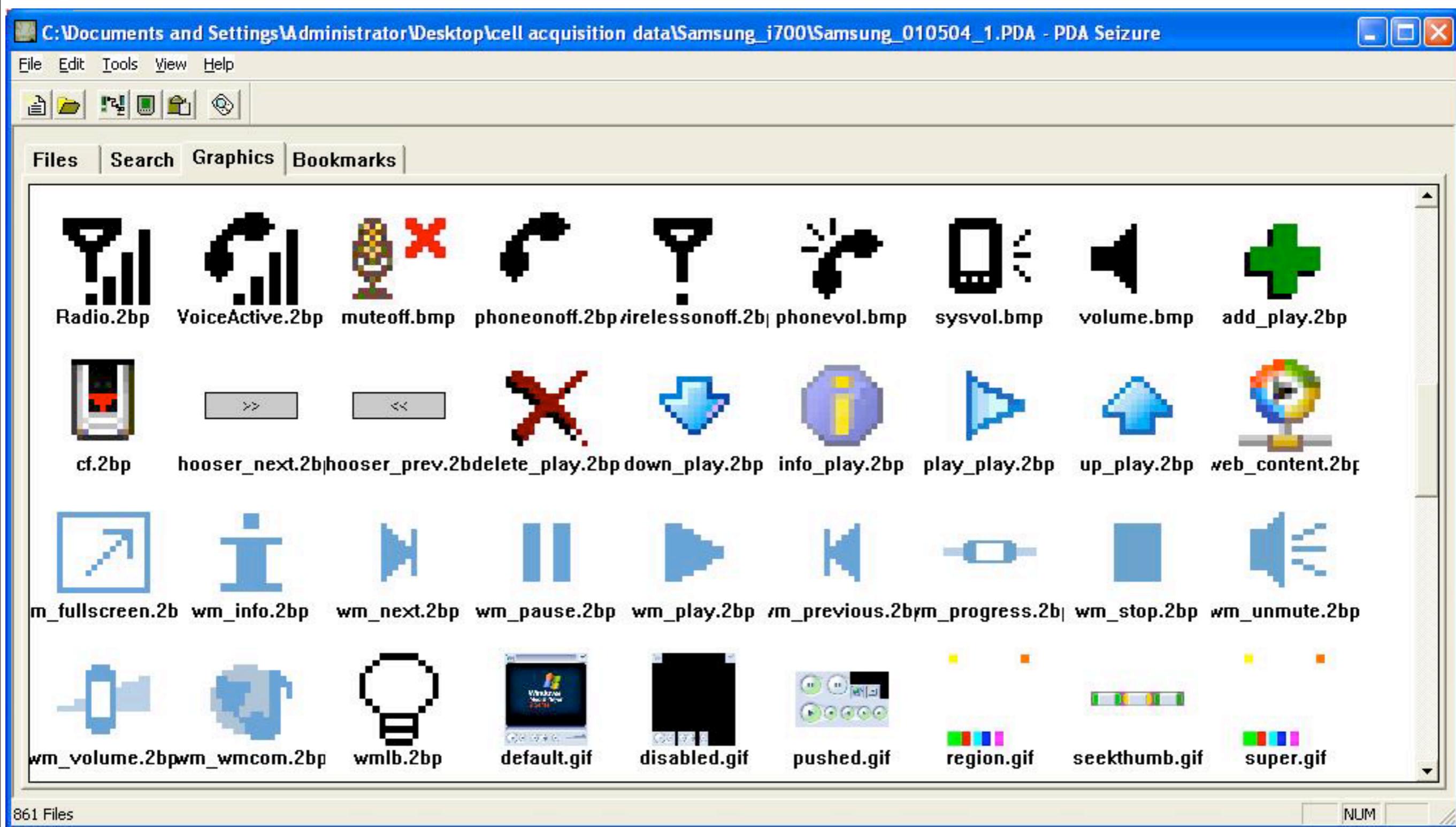
```

...@...H.....:...t...(. ....@.....:.....:.....(.....:.....:.....(.....l.....
.....c.a.r.t.m.a.n.@.s.o.u.t.h.p.a.r.k..n.e.t...(.1.2.3.) .4.5.6.-.7.8.9.0....C.a.r.t.m.a.n.,. .E.r.i.c...S.o.u.t.h. .P.a.r.k....E.r.
i.c....C.a.r.t.m.a.n...T.h.i.r.d. .G.r.a.d.e.r.....:.....H...@.....(.....:.....0.....:.....8.6.7.
-.5.3.0.9...(.R.i.c.k.a.y.e.r.s...R.i.c.k.a.y.e.r.s.....(.....l.....c.a.r.t.m.a.n.@.s.o.u.t.h.p.a.r.k..n.e.t...(.1.2.3.) .4.
5.6.-.7.8.9.0....C.a.r.t.m.a.n.,. .E.r.i.c...S.o.u.t.h. .P.a.r.k....E.r.i.c....C.a.r.t.m.a.n...T.h.i...@.....H.....:.....(.....
.@H.....d.....:.....0.....x.....:.....L.....:.....X.....:.....h...-5.....9.....i.c....y.....R.h.o.m.e.r.@.d.u.f.f..c.o.m.
....(.9.8.7.) .6.5.4.-.3.2.1.0...o.S.i.m.p.s.o.n.,. .H.o.m.e.r...3.T.h.e. .S.i.m.p.s.o.n.s...a.H.o.m.e.r...S.i.m.p.s.o.n...N.u.c.l.e.a.r.
.S.a.f.e.t.y. .I.n.s.p.e.c.t.o.r...h.
    
```

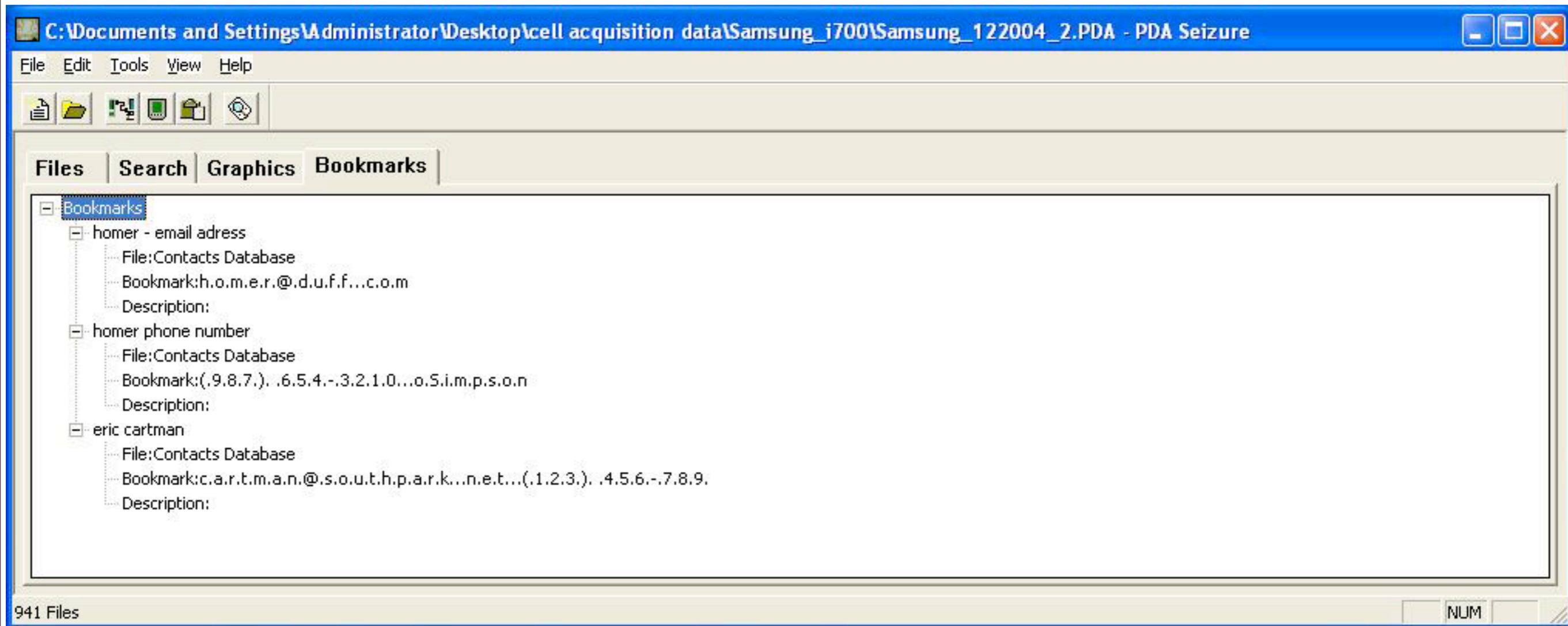
File Name	Text
Contacts Databasei.c...bÿÿ.....R.h.o.m.e.r.@.d.u.f.f..c.o.m...bÿ(9.8.7.) .6.5.4.
Contacts Database	.) .6.5.4.-.3.2.1.0...o.S.i.m.p.s.o.n.,. .H.o.m.e.r...3.T.h.e. .S.i.m.p.s.
Contacts Database	.0...o.S.i.m.p.s.o.n.,. .H.o.m.e.r...3.T.h.e. .S.i.m.p.s.o.n.s...a.H.o.m.e.
Contacts Database	. .H.o.m.e.r...3.T.h.e. .S.i.m.p.s.o.n.s...a.H.o.m.e.r...S.i.m.p.s.o.n...N.
Contacts Database	.e. .S.i.m.p.s.o.n.s...a.H.o.m.e.r...S.i.m.p.s.o.n...N.u.c.l.e.a.r. .S.a.f.
Contacts Database	.s.o.n.s...a.H.o.m.e.r...S.i.m.p.s.o.n...N.u.c.l.e.a.r. .S.a.f.e.t.y. .I.n.

Ready NUM

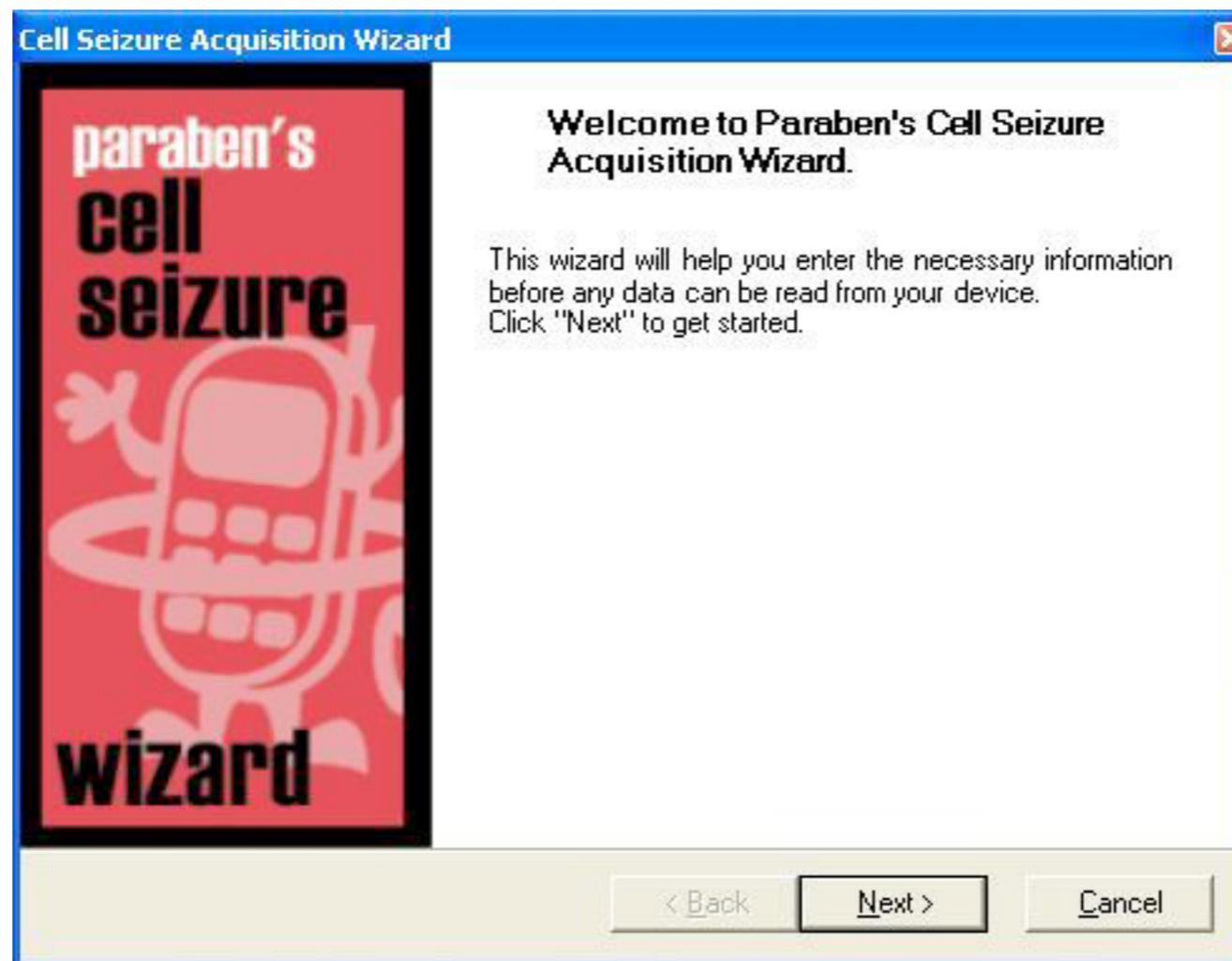
Paraben's PDA Seizure



Paraben's PDA Seizure



Paraben's Cell Seizure



Paraben's Cell Seizure

The screenshot displays the Paraben's Cell Seizure application interface. The main window shows a workspace with a tree view on the left and a data table on the right. The tree view is expanded to show the 'Phonebook (26)' folder. The data table lists various phonebook entries with columns for Location, Number, and Name. A search dialog box is open in the foreground, showing the search results for 'homer simpson'.

Location	Number	Name
Phone memory	"9784653210"	Homer Simpson
Phone&Sim	"9784653210"	Homer Simpson
Emergency numbers	""	@
Emergency numbers	""	@
Emergency numbers	""	@

Search - 1/3 values were found

Text: homer simpson

Hex: 68 6F 6D 65 72 20 73 69 6D 70 7

In:

- Workspace
- Current device
- Current selection

Whole word

Match case

Buttons: Find, Cancel, Close, Add To Bookmarks, First, Previous, Next, Last



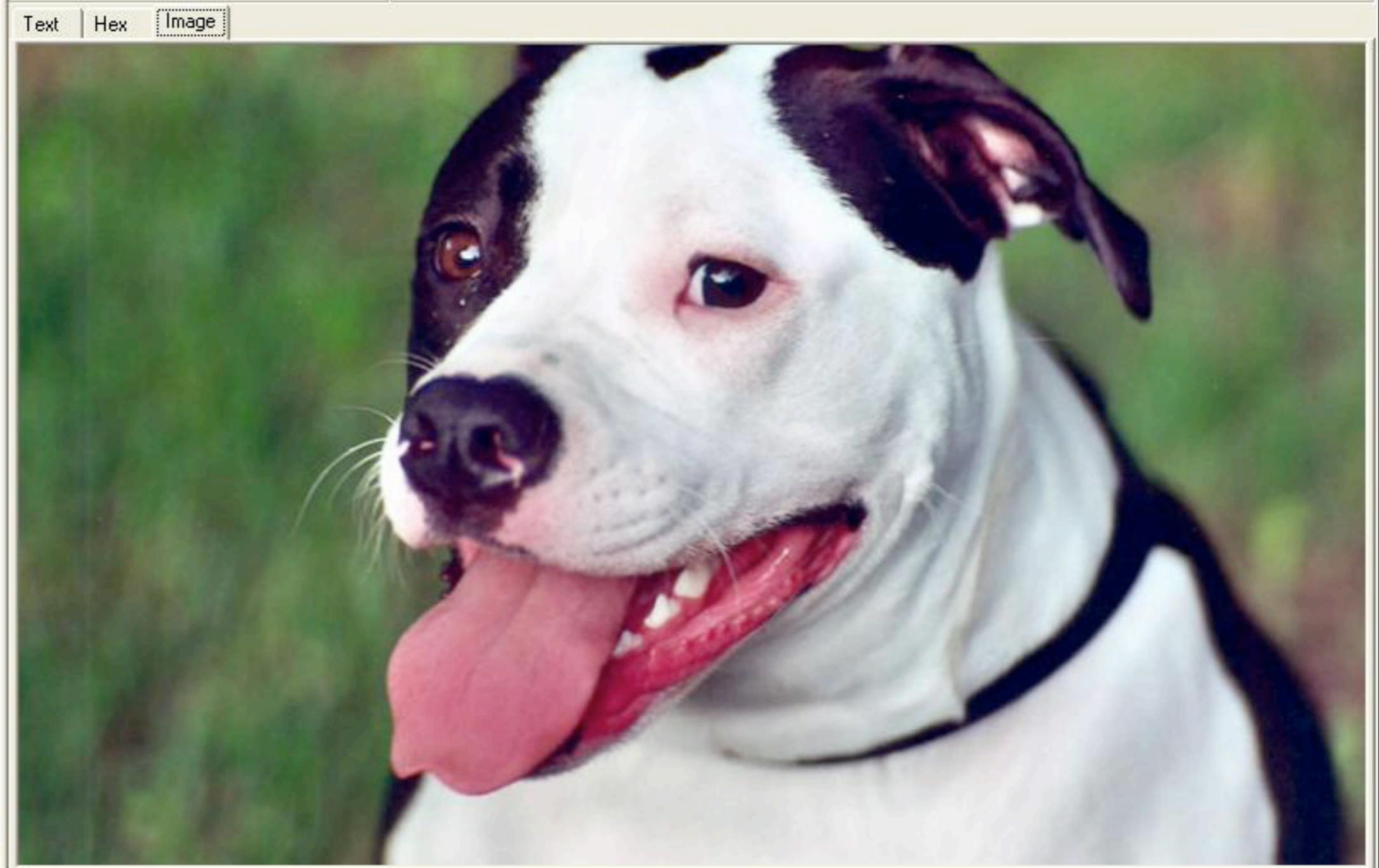
Workspace

View

- 033 - Heavenly (1)
- 035 - Just jazzy (1)
- 037 - Mountain (1)
- 039 - Robotique (1)
- 041 - Songette (1)
- 043 - test files (1)
- 045 - Clouds.jpg (1)
- 047 - Sunflower.jpg (1)
- 049 - Sunset.jpg (1)
- 051 - Coffee.jpg (1)
- 053 - Travel.jpg (1)
- 055 - Heart.jpg (1)
- 057 - 661FCAD 661F
- 059 - Clip-art04.gif (1)
- 061 - Clip-art06.gif (1)
- 063 - Clip-art08.gif (1)
- 065 - Clip-art10.gif (1)
- 067 - Frame02.gif (1)
- 069 - Frame04.gif (1)
- 071 - Frame06.gif (1)
- 073 - Frame08.gif (1)
- 075 - Frame10.gif (1)
- 077 - Cnv_en_zh-CN
- 079 - Boun_en_zh-Ct
- 081 - Boun_en_zh-Ct
- 083 - Chep_en_zh-Ct
- 085 - Pmgr_en_zh-Ct
- 087 - Pmgr_en_zh-Ct
- 089 - emma-girl.jpg (1)
- 091 - Beer.png (1)
- 093 - emma-girl.jpg (1)
- 095 - exe_file.doc (1)
- 097 - forensics.pdf (1)
- 099 - homer.gif (1)
- 101 - test1.rar (1)
- 103 - test3.exe (1)
- 105 - test5.tar (1)

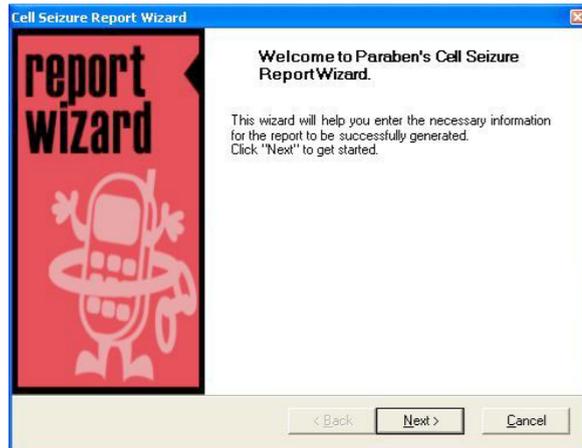
GoTo: Find Text:

Len/Pos: 0x0000e58c / 0x00000000 Hex:



0x0000e58c / 0x00000000

Paraben's Cell Seizure Report Wizard



```
Paraben's Cell Seizure Exported Workspace
Motorola V.series 66

Properties
Name-----Value-----
Manufacturer : Motorola :
Model : V.series 66 :
Serial number : IMEI449276812531841.... :
MD5 : 47bae0d246ffa06a341b3c62ef61c7ff :
Phonebook
Location-----Number-----Name-----
Phone memory : "9784653210" : Homer Simpson :
Phone&Sim : "9784653210" : Homer Simpson :
Properties
Name-----Value-----
MD5 : d41d8cd98f00b204e9800998ecf8427e :
SMS
Number-----Status-----Date/Time-----Message-----
"2404016148" : "STO UNSENT" : : 体 :
Properties
Name-----Value-----
MD5 : d41d8cd98f00b204e9800998ecf8427e :
Calls History
Name-----Number-----Direction-----
Homer Simpsons/W : "9874653210" : Dialed calls :
: "301975XXXX" : Dialed calls :
: "301975XXXX" : Dialed calls :
Properties
Name-----Value-----
MD5 : d41d8cd98f00b204e9800998ecf8427e :
Datebook
Ricks birthday : 0 : 0 : 2000-01-30 00:00 : 1440 : : non reoccurring :
Properties
Bookmarks Homer Simpson : Homer Simpson Datebook entry : Ricks birthday
```

Cell Phone Forensics: References & Resources

Guidelines on Cell Phone Forensics (NIST SP 800-101)

- August 2006
- <http://csrc.nist.gov/publications/drafts/Draft-SP800-101.pdf>

Cell Phone Forensic Tools: An Overview and Analysis (NISTIR 7250)

- <http://csrc.nist.gov/publications/nistir/nistir-7250.pdf>

PDA Forensic Tools: An Overview and Analysis (NISTIR 7100)

- <http://csrc.nist.gov/publications/nistir/nistir-7100-PDAForensics.pdf>

```
if(dirlist.size()==0){
    if(argc!=2){
        fprintf(stderr,"Please specify a directory or just two AFF files.\n\n");
        usage();
    }
    /* Must be copying from file1 to file2. Make sure file2 does not exist */
    if(access(argv[1],R_OK)==0){
        errx(1,"File exists: %s\n",argv[1]);
    }

    vector<string> outfiles;
    outfiles.push_back(argv[1]);
    return afcopy(argv[0],outfiles);
}
```

Software Forensics

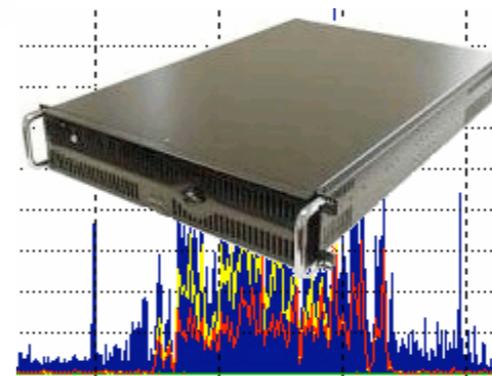
Who authored a program?
Are two programs similar?
How old is a program?

Tutorial Roadmap...

- ✓ Introduction
- ✓ The Forensic Process
- ✓ Legal Standards
- ✓ Specific Forensic Techniques

- Disk Forensics
- Network Forensics
- Document Forensics
- Memory Forensics
- Cell Phone Forensics
- Software Forensics

4. Anti-Forensics



```
printf("%d, %f", i, f);  
    i++; f+=3.0;  
    g = fmod(f,i);
```

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 hampered by the Intelligence Community's dependence on having an official U.S. presence in-country to monitor clandestine HUMINT collection efforts.

(b) When UN inspectors departed Iraq, the placement of HUMINT agents and the development of unaffiliated 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 risk 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.

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 was hard to maintain... it takes a rare officer who can go in... and survive scrutiny... for a long time." The Committee agrees that such operations are difficult and dangerous, but they should be within the scope of the CIA's activities and capabilities. Some CIA officials have repeatedly told the Committee that a significant increase in funding and personnel will be required to enable the CIA to possess sufficient HUMINT assets to prevent 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.

(c) 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 foreign 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 -



Anti-Forensics: Techniques, Detection and Countermeasures

What is Anti-Forensics?

Computer Forensics: *“Scientific Knowledge for collecting, analyzing, and presenting evidence to the courts” (USCERT 2005)*

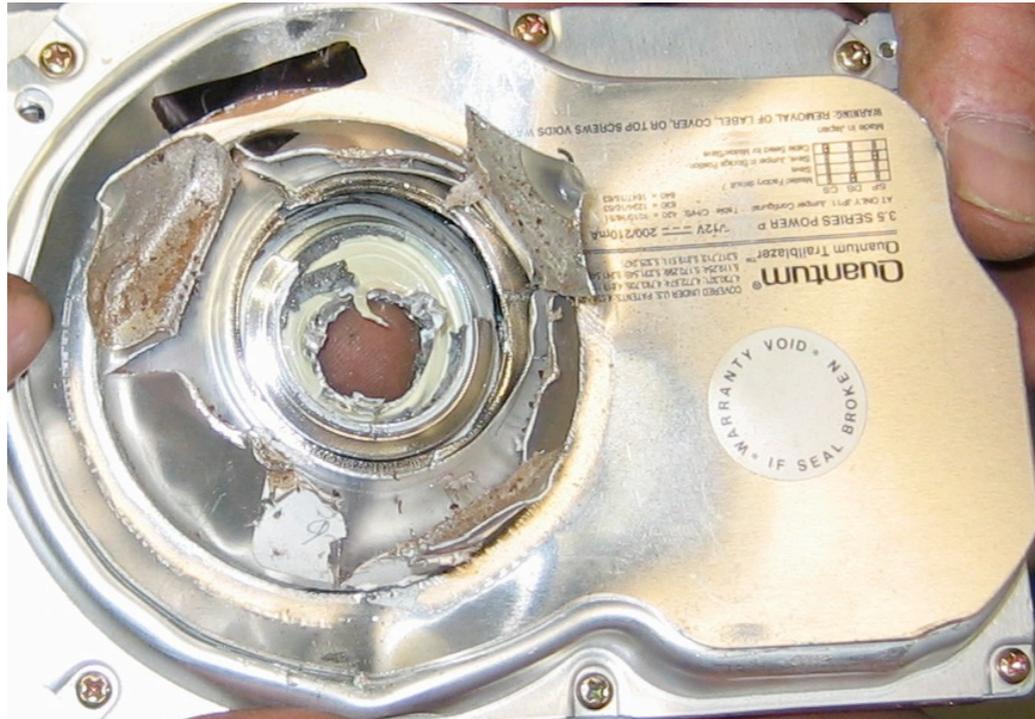
Anti-Forensics: *tools and techniques that frustrate forensic tools, investigations and investigators*

Goals of Anti-Forensics:

- *Avoiding detection*
- *Disrupting information collection*
- *Increasing the examiner’s time*
- *Casting doubt on a forensic report or testimony (Liu and Brown, 2006)*

- *Forcing a tool to reveal its presence*
- *Subverting the tool — using it to attack the examiner or organization*
- *Leaving no evidence that the AF tool has been run*

Physical destruction makes forensic recovery impossible.



One traditional Anti-Forensic technique is to overwrite or otherwise destroy data.

Overwriting: Eliminate data or metadata (e.g. disk sanitizers, Microsoft Word metadata “washers,” timestamp eliminators.)

Disk Sanitizers; Free Space Sanitizers; File Shredders

- Microsoft **Remove Hidden Data Tool**; **cipher.exe**; **ccleaner**

Metadata Erasers

- Example: **timestomp**

Hard problem: *What should be overwritten?*

Anti-Forensic tools can hide data with cryptography or steganography.

Cryptographic File Systems (EFS, TrueCrypt)

Encrypted Network Protocols (SSL, SSH, Onion Routing*)

Program Packers (PECompact, Burneye) & Rootkits

Steganography

Data Hiding in File System Structures

- Slacker — Hides data in slack space
- FragFS — Hides in NTFS Master File Table
- RuneFS — Stores data in “bad blocks”
- KY FS — Stores data in directories
- Data Mule FS — Stores in inode reserved space
- Host Protected Areas & Device Configuration Overlay

*Onion routing also protects from traffic analysis

Anti-Forensics 3: Minimizing the Footprint

Overwriting and Data Hiding are *easy to detect*.

- Tools leave tell-tale signs; examiners know what to look for.
- Statistical properties are different after data is overwritten or hidden.

AF tools that minimize footprint avoiding leaving traces for later analysis.

- Memory injection and syscall proxying
- Live CDs, Bootable USB Tokens
- Virtual Machines
- Anonymous Identities and Storage

(don't worry; we have slides for each of these)

Memory Injection and Userland Execve: Running a program without loading the code.

Memory Injection loads code without having the code on the disk.

- **Buffer overflow** exploits — run code supplied as (oversized) input

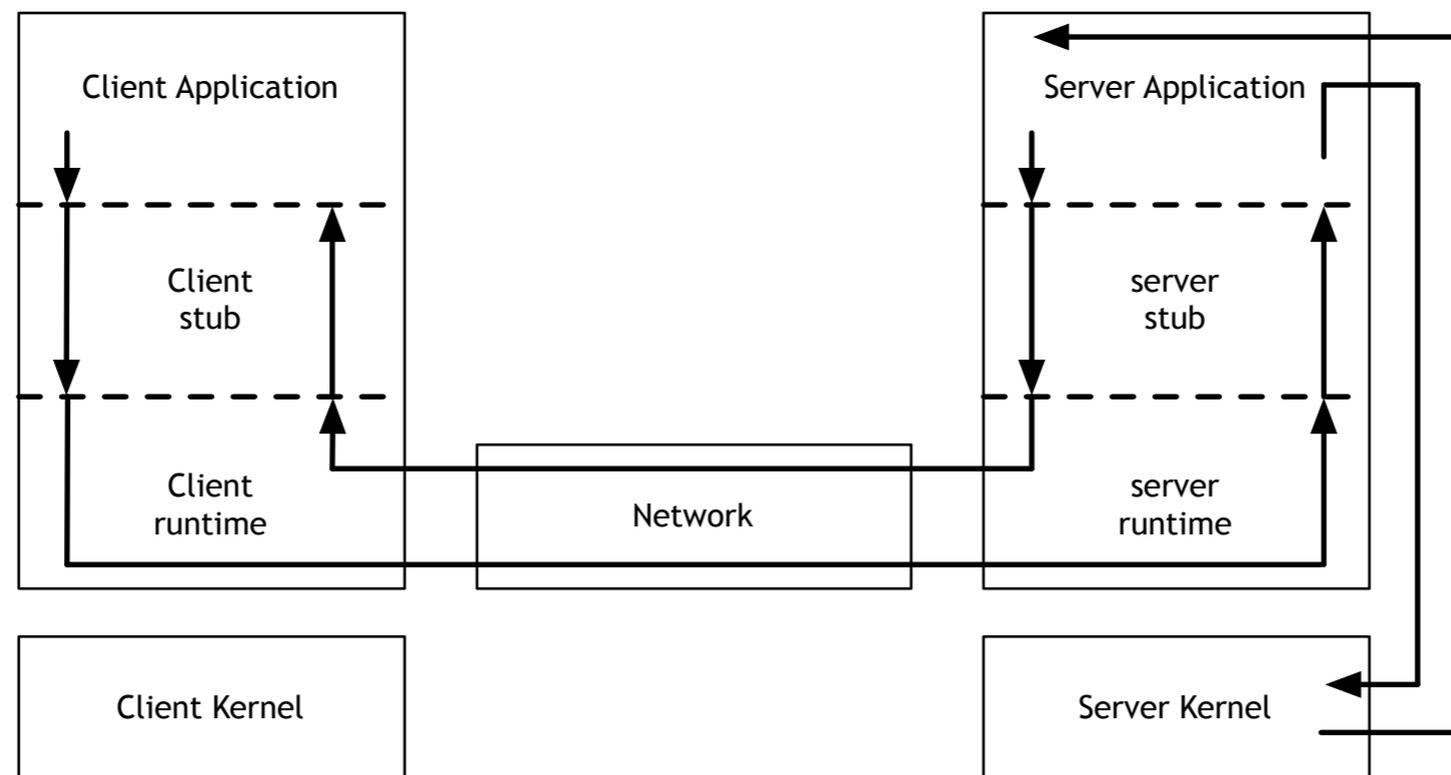
Userland Execve

- Runs program without using `execve()`
- Bypasses logging and access control
- Works with code from disk or read from network

Syscall proxying: Running a program without the code!

Syscall Proxying

- Program runs on one computer, syscalls executed on another.
- Program not available for analysis
- May generate a lot of network traffic
- Developed by Core Security; used in **Impact**



Live CDs, Bootable USB Tokens, Virtual Machines: Running code without leaving a trace.

Most forensic information is left in the file system of the running computer.

These approaches keep the attacker's file system segregated:

- In RAM (CDs & Bootable USB Tokens)
- In the Virtual Machine file (where it can be securely deleted)



Anonymous Identities and Storage:

The attacker's data may be anywhere.

Attackers have long made use of anonymous e-mail accounts. Today these accounts are far more powerful.

- Yahoo and GMail both have 2GB of storage
- APIs allow this storage to be used as if it were a file system

Amazon's Elastic Compute Cloud (EC2) and Simple Storage Service (S3) provide high-capability, little-patrolled services to anyone with a credit card

- EC2: 10 ¢/CPU hour (Xen-based virtual machines)
- S3: 10 ¢/GB-Month

With BGP, it's possible to have "anonymous IP addresses."

1. Announce BGP route
2. Conduct attack
3. Withdraw BGP address

Being used by spammers today
(<http://www.nanog.org/mtg-0602/pdf/feamster.pdf>)

Attacking the Investigator: AF techniques that exploit CFT bugs.

Craft packets to exploit buffer-overflow bugs in network monitoring programs like **tcpdump**, **snort** and **ethereal**.

Create files that cause EnCase to crash.

Successful attacks provide:

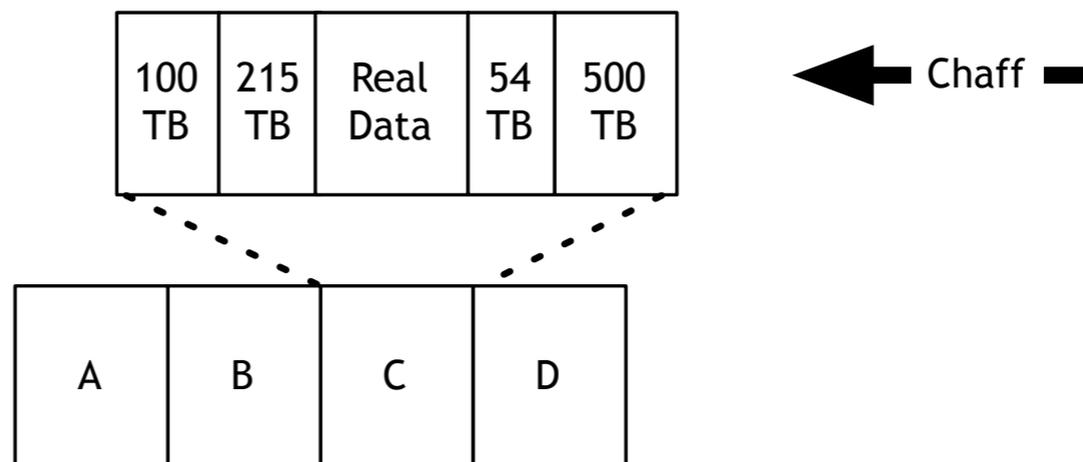
- ➡ Ability to run code on the forensic appliance
- ➡ Erase collected evidence
- ➡ Break the investigative software
- ➡ Leak information about the analyst or the investigation
- ➡ Implicate the investigator

Attacking the Investigator: Denial-of-Service Attacks against the CFT

Any CFT resource whose use is determined by input can be overwhelmed.

- Create millions of files or identities
- Overwhelm the logging facility
- Compression bombs — 42.zip

The clever adversary will combine this **chaff** with real data, e.g.:



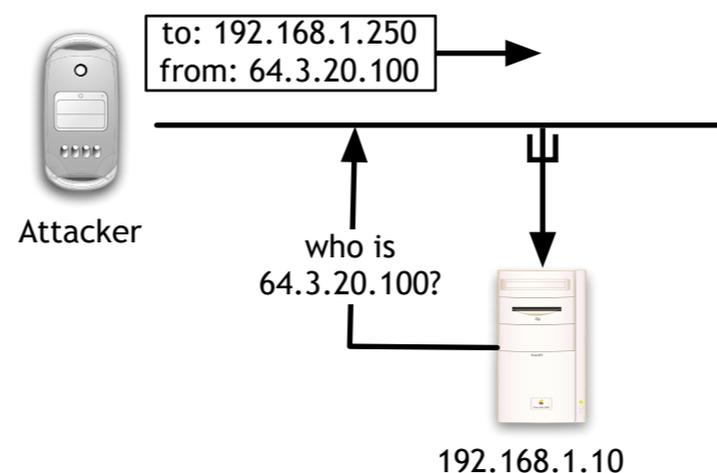
Anti-Forensic Tools can detect Computer Forensic Tools: cat-and-mouse.

SMART (Self-Monitoring, Analysis and Reporting Technology) drives report:

- Total number of power cycles
- Total time hard drive has been on

Network Forensics can be detected with:

- Hosts in “promiscuous” mode responding differently
 - to PINGs.
 - to malformed packets
 - to ARPs
- Hosts responding to traffic not intended to them (MAC vs. IP address)
- Reverse DNS queries for packets sent to unused IP addresses



Countermeasures for Anti-Forensics

Improve the tools — many CFTs are poorly written.

Save data where the attacker can't get at it:

- Log hosts
- CD-Rs

Develop new tools:

- Defeat encrypted file systems with keyloggers.
- Augment network sniffers with traffic analysis

Research directions in Computer Forensics

Environmental Data Survey Projects

- Phone systems
- Hard drives & data storage devices
- Network hosts and traffic

Theory and Algorithm Development:

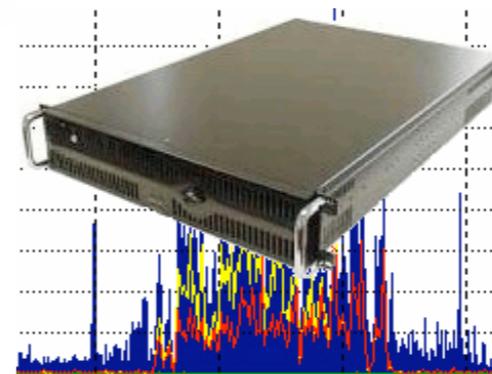
- Theoretical basis to forensics (Brian Carrier 2006 PhD)
- Cross-Drive Analysis (Garfinkel)
- Carving Fragmented Objects with Validation

Tool Development

- Easy-to-use tools
- Batch tools
- Data correlation

Tutorial Roadmap...

- ✓ Introduction
- ✓ The Forensic Process
- ✓ Legal Standards
- ✓ Specific Forensic Techniques
 - Disk Forensics
 - Network Forensics
 - Document Forensics
 - Memory Forensics
 - Cell Phone Forensics
 - Software Forensics
- ✓ Anti-Forensics



```
printf("%d, %f", i, f);  
    i++; f+=3.0;  
    g = fmod(f,i);
```

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 blood society like Iraq prior to Operation Iraqi Freedom were hampered by the Intelligence Community's dependence on having an official U.S. presence in-country to monitor clandestine HUMINT collection efforts.

(b) When UN inspectors departed Iraq, the placement of HUMINT agents and the development of unaffiliated 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 risk 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.

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 was hard to maintain... it takes a rare officer who can go in... and survive scrutiny... for a long time." The Committee agrees that such operations are difficult and dangerous, but they should be within the scope of the CIA's activities and capabilities. Some CIA officials have repeatedly told the Committee that a significant increase in funding and personnel will be required to enable the CIA to possess difficult HUMINT assets similar to those 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.

(c) 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 foreign 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 -

Conclusion

Forensic analysis is a growth area.

Being a practitioner is hard:

- Many skills
- Many tools
- In-depth knowledge of many different systems

Conclusion

Forensic analysis is a growth area.

Being a practitioner is hard:

- Many skills
- Many tools
- In-depth knowledge of many different systems

**Please fill out the Tutorial Evaluation:
<http://www.usenix.org/usercon07tutevals/>**

Other Resources

US DoJ Computer Crime & Intellectual Property Section:

- <http://www.cybercrime.gov/>

Wikis:

- <http://www.forensicswiki.org/>
- <http://www.forensicwiki.com/>

Blogs and Communities:

- <http://computer.forensikblog.de/en/>

Link Farms

- <http://staff.washington.edu/dittrich/forensics.html>
- <http://faculty.ncwc.edu/toconnor/426/426links.htm>