

Data Recovery

Mitchell Dawson
Jon Davis

Chris Forgie
Steve Tauber

CSSE 592/492 Computer Forensics
May 7th, 2003

Overview

- What is Data Recovery?
- How can it be used?
- Techniques
 - Recovery Methods
 - Secure Deletion
 - Private vs. Government services
 - Software vs. Hardware Solutions
- What can you do?

What is data recovery?

- Retrieving deleted/inaccessible data from electronic storage media (hard drives, removable media, optical devices, etc...)
- Typical causes of loss include:
 - Electro-mechanical Failure
 - Natural Disaster
 - Computer Virus
 - Data Corruption
 - Computer Crime
 - Human Error
- Example
 - <http://www.drivesavers.com/museum/qtpopisdn.html>

Cases of Recovery



FIRE

Found after a fire destroyed a 100 year old home – All data Recovered



CRUSHED

A bus runs over a laptop
– All data recovered



SOAKED

PowerBook trapped underwater for two days – All data recovered

Uses of data recovery

- Average User:
 - Recover important lost files
 - Keep your private information private
- Law enforcement:
 - Locate illegal data
 - Restore deleted/overwritten information.
 - Prosecute criminals based on discovered data

Software Recovery of data

- Generally only restore data not yet overwritten.
- Do not work on physically damaged drives
- Undelete Pro, EasyRecovery, Proliant, Novanet, etc.
- Prices range from Free-1000
- Example: dd on linux used on corrupt floppies

Private Recovery Services

- Many private companies offer quick, secure, and confidential data recovery:
 - Computer Disk Service <http://www.compdisk.com>
 - 20 GB from \$195.00
 - 46 GB and up – from \$895.00
 - Action Front <http://www.datarec.com/>
 - External cases - \$500 to \$1500
 - Internal cases -\$2500 to \$4000 for a single hard drive
 - Critical Response services start at \$5,000.
 - Data Recovery Services - <http://www.datarecovery.net/>

Recovery Methods

- Hidden files
- Recycle bin
- Unerase wizards
- Assorted commercial programs
- Ferrofluid
 - Coat surface of disk
 - Check with optical microscope
 - Does not work for more recent hard drives
- More recently...

Recovery Methods

- When data is written – the head sets the polarity of most, but not all, of the magnetic domains
- The actual effect of overwriting a bit is closer to obtaining a 0.95 when a zero is overwritten by a one, and a 1.05 when a one is overwritten with a one.
 - Normal equipment will read both these values as ones
 - However, using specialized equipment, it is possible to work out what the previous “layers” contained
- Steps include
 - Reading the signal from the analog head electronic with a high-quality digital oscilloscope
 - Downloading the sampled waveform to a PC
 - Analyzing it in software to recover the previously recorded signal.

Recovery Methods

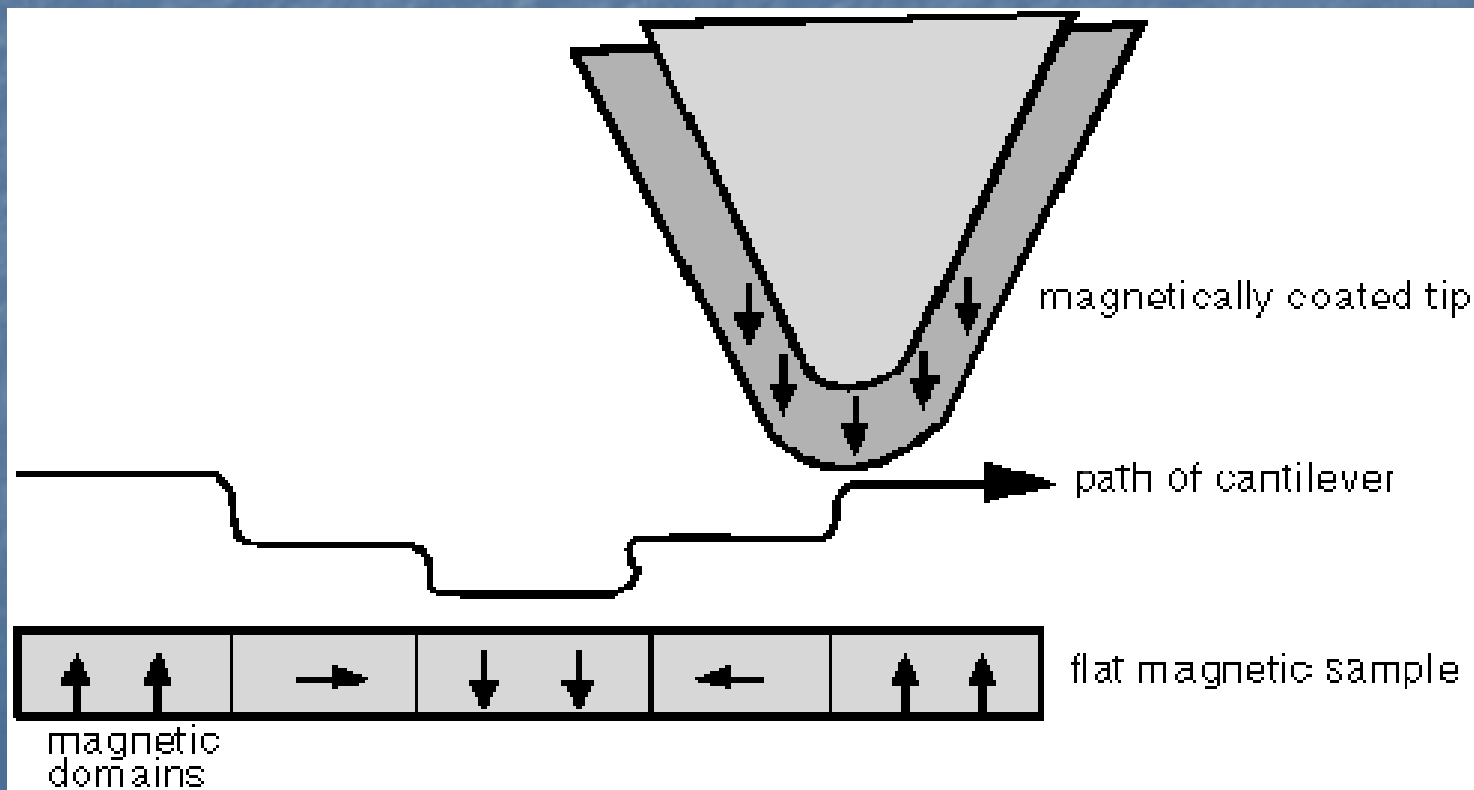
- Scanning Probe Microscopy (SPM)
 - Uses a sharp magnetic tip attached to a flexible cantilever placed close to the surface to be analyzed, where it interacts with the stray field emanating from the sample to produce a topographic view of the surface
 - Reasonably capable SPM can be built for about US\$1400, using a PC as a controller
 - Thousands in use today

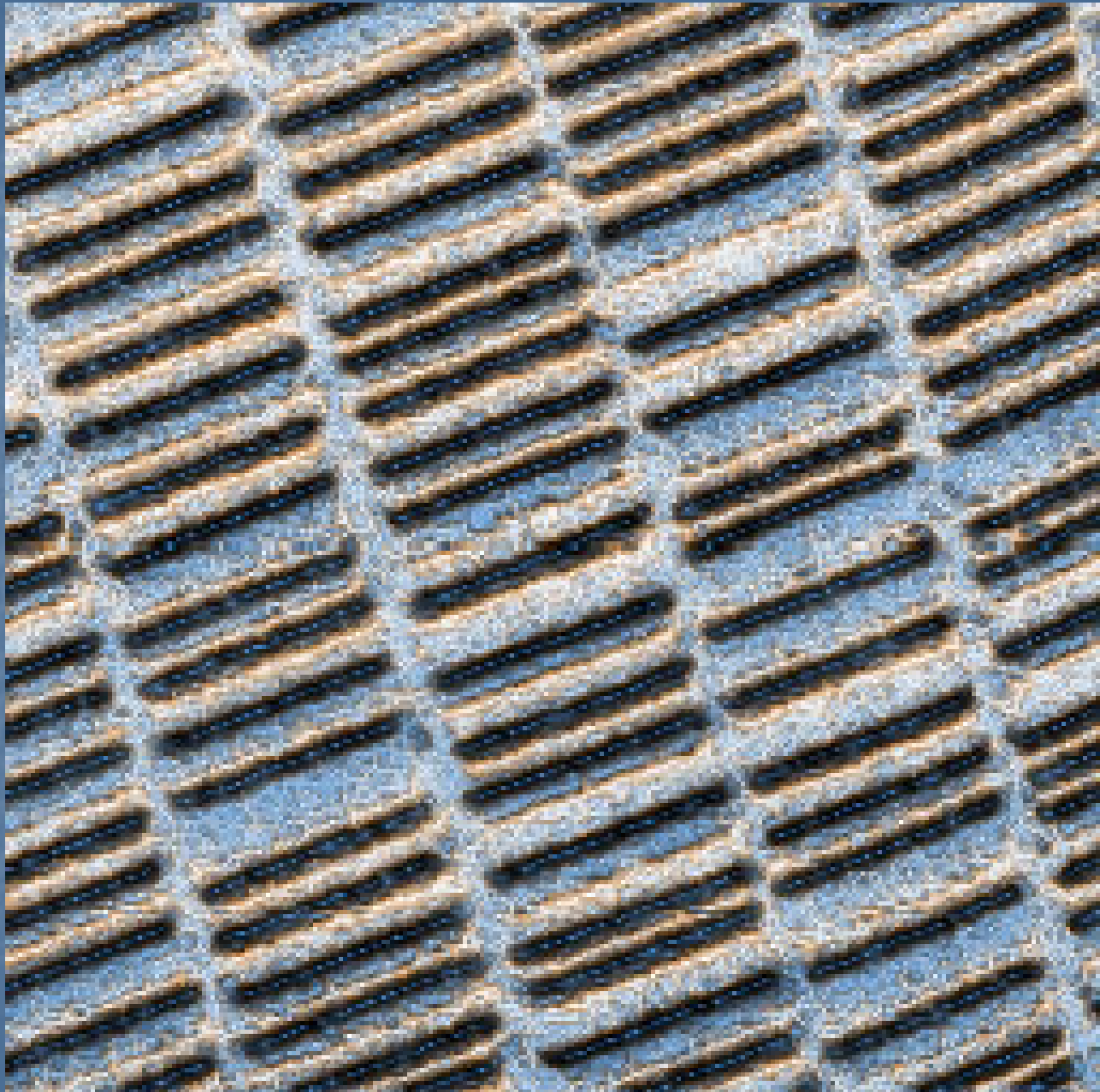
Recovery Methods

- Magnetic force microscopy (MFM)
 - Recent technique for imaging magnetization patterns with high resolution and minimal sample preparation.
 - Derived from scanning probe microscopy (SPM)
 - Uses a sharp magnetic tip attached to a flexible cantilever placed close to the surface to be analyzed where it interacts with the stray magnetic field
 - An image of the field at the surface is formed by moving the tip across the surface and measuring the force (or force gradient) as a function of position. The strength of the interaction is measured by monitoring the position of the cantilever using an optical interferometer.

Recovery Methods

- Magnetic force microscopy (MFM)





Recovery Methods

■ Using MFM:

- Techniques can detect data by looking at the minute sampling region to distinctly detect the remnant magnetization at the track edges.
- Detectable old data will still be present beside the new data on the track which is usually ignored
- In conjunction with software, MFM can be calibrated to see past various kinds of data loss/removal. Can also do automated data recovery.
- It turns out that each track contains an image of everything ever written to it, but that the contribution from each "layer" gets progressively smaller the further back it was made.

How to Avoid Data Recovery

- Companies, agencies, or individuals may want to ensure their data cannot be recovered.
- Simple deletion is not good enough.
- Faced with techniques such as MFM, truly deleting data from magnetic media is very difficult

Secure Deletion: Government Standards

- Department of Justice:
 - DoD 5220.22-M – Type 1 degausser, followed by type 2 degausser, then three data overwrites (character, its complement, random)
- Problems with government standards
 - Often old and predate newer techniques for both recording and recovering data.
 - Predate higher recording densities of modern drives, the adoption of sophisticated channel coding techniques, and the use of MFM.
 - Government standard may in fact be understated to fool opposing intelligence agencies.

Secure Deletion Techniques

- Degaussing
 - Process in which the media is returned to its initial state
 - Coercivity – Amount of magnetic field necessary to reduce the magnetic induction to zero. (measured in Oersteds)
 - Effectively erasing a medium to the extent that data recovery is uneconomical requires a magnetic force ~5x the coercivity.
 - US Government guidelines on media coercivity:
 - Class 1: 350 Oe coercivity or less
 - Class 2: 350-750 Oe coercivity.
 - Class 3: over 750 Oe coercivity
 - Degaussers are available for classes 1 and 2. None known for **fully** degaussing class 3 media.

Techniques

Secure Deletion – Avoiding Recovery

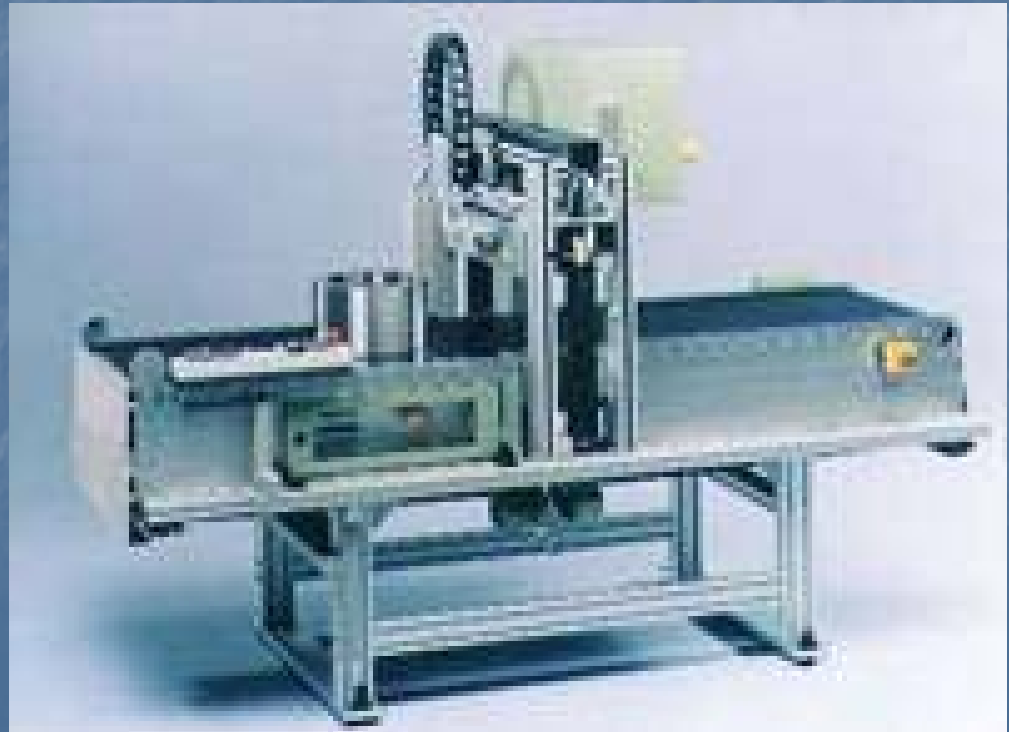
Typical Media Coercivity Figures	
Medium	Coercivity
5.25" 360K floppy disk	300 Oe
5.25" 1.2M floppy disk	675 Oe
3.5" 720K floppy disk	300 Oe
3.5" 1.44M floppy disk	700 Oe
3.5" 2.88M floppy disk	750 Oe
3.5" 21M floptical disk	750 Oe
Older (1980's) hard disks	900-1400 Oe
Newer (1990's) hard disks	1400-2200 Oe
1/2" magnetic tape	300 Oe
1/4" QIC tape	550 Oe
8 mm metallic particle tape	1500 Oe

Commercial Degaussers



Type I

Type II/III



Deletion Techniques

- Technique 2: Multiple Overwrites
- Use an overwrite scheme
 - Flip each magnetic domain on the disk back and forth as much as possible
 - Overwrite in alternating patterns to expose it to an oscillating magnetic field.
 - Overwrite with “junk” data several times
- Use the lowest frequency possible for overwrites
 - Penetrates deeper into the recording medium

Deletion Techniques

- Peter Guttman's overwrite scheme:
 - Meant to defeat all possible recovery techniques (MFM, etc)
 - Specifies 35 different overwrites
 - Not all overwrites are needed if targeting specific recovery method (i.e. MFM)

Overwrite Data				
Pass No.	Data Written	Encoding Scheme Targeted		
1 - 4	Random			
5	01010101 01010101 01010101 0x55	(1,7)RLL		MFM
6	10101010 10101010 10101010 0xAA	(1,7)RLL		MFM
7	10010010 01001001 00100100 0x92 0x49 0x24		(2,7)RLL	MFM
8	01001001 00100100 10010010 0x49 0x24 0x92		(2,7)RLL	MFM
9	00100100 10010010 01001001 0x24 0x92 0x49		(2,7)RLL	MFM
10	00000000 00000000 00000000 0x00	(1,7)RLL	(2,7)RLL	
11	00010001 00010001 00010001 0x11	(1,7)RLL		
12	00100010 00100010 00100010 0x22	(1,7)RLL		
13	00110011 00110011 00110011 0x33	(1,7)RLL	(2,7)RLL	
14	01000100 01000100 01000100 0x44	(1,7)RLL		
15	01010101 01010101 01010101 0x55	(1,7)RLL		MFM
16	01100110 01100110 01100110 0x66	(1,7)RLL	(2,7)RLL	
17	01110111 01110111 01110111 0x77	(1,7)RLL		
18	10001000 10001000 10001000 0x88	(1,7)RLL		
19	10011001 10011001 10011001 0x99	(1,7)RLL	(2,7)RLL	
20	10101010 10101010 10101010 0xAA	(1,7)RLL	MFM	
21	10111011 10111011 10111011 0xBB	(1,7)RLL		
22	11001100 11001100 11001100 0xCC	(1,7)RLL	(2,7)RLL	
23	11011101 11011101 11011101 0xDD	(1,7)RLL		
24	11101110 11101110 11101110 0xEE	(1,7)RLL		
25	11111111 11111111 11111111 0xFF	(1,7)RLL	(2,7)RLL	
26	10010010 01001001 00100100 0x92 0x49 0x24		(2,7)RLL	MFM
27	01001001 00100100 10010010 0x49 0x24 0x92		(2,7)RLL	MFM
28	00100100 10010010 01001001 0x24 0x92 0x49		(2,7)RLL	MFM
29	01101101 10110110 11011011 0x6D 0xB6 0xDB		(2,7)RLL	
30	10110110 11011011 01101101 0xB6 0xDB 0x6D		(2,7)RLL	
31	11011011 01101101 10110110 0xDB 0x6D 0xB6		(2,7)RLL	
32-35	Random			

Deletion Techniques

- Extremely Extreme Physical Destruction
 - Chainsaws
 - Sledge hammers
 - Drop in a volcano
 - Place on apex of a nuclear warhead
 - Multiple rounds from a high caliber firearm
- Hard Drivers are tougher than you think

What can you do?

To reliably remove files?

- Not Much - absolutely secure is very difficult given methods out today
- Make it impractical or extremely expensive to recover

In the News

- After buying 158 drives, ZDNet Finds:
 - Over 5,000 credit card numbers
 - Medical records
 - Detailed personal and corporate financial information
 - Personal Emails
 - Gigs of pornography
- Pennsylvania sold used computer that contained information about state employees
- A woman in Nevada bought a used computer which contained the prescription records of over 2,000 customers of an Arizona pharmacy.

QUESTIONS?



Resources

- http://www.geocities.com/spezzin_grazer/cap-4/cap4.htm
- http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html
- <http://sfgate.com>
- <http://www.executivesoftware.com>
- <http://www.softwareshef.com>
- <http://www.geek.com/news/>
- <http://www slashdot.com>
- <http://www.compdisk.com>