Digital Forensics

Finding information that has been lost...

BJ Gleason

Digital Forensics

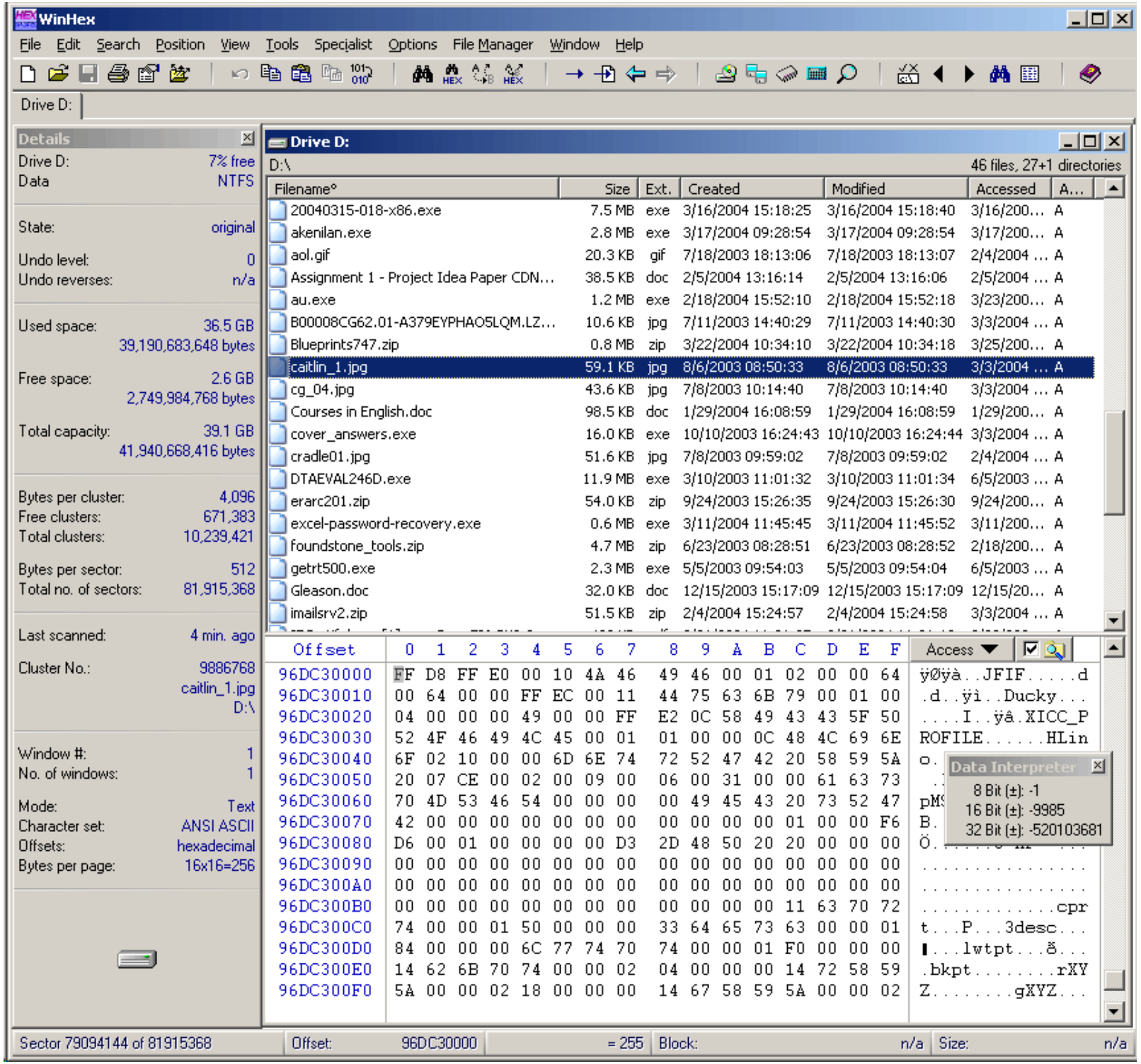
Collecting
Preserving
Analyzing
Reconstructing

Evidence from a Crime
  Where a computer was used

Digging Deep for Clues...

Your Shovel

WinHex



Let's Start with a blank floppy

Create a file

Overwrite it

Delete it

Format it (Quick)

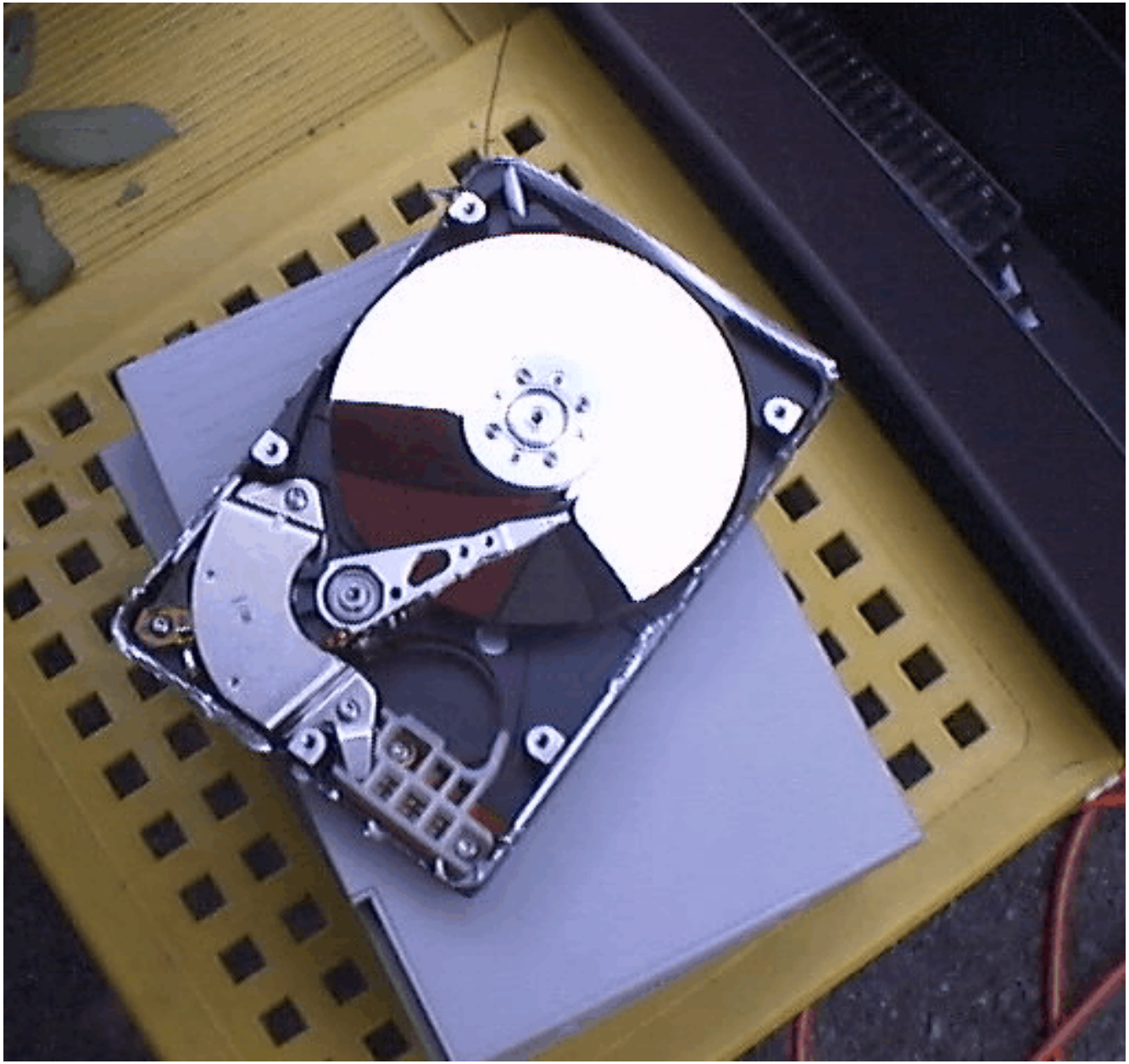
Wiping Drives

With all the problems we had deleting file from the disk, this program will do it for us.

Delete Files
Wipe Free Space, Slack Space, Swap

Wipe Drive - DOS utility Wipe HD
BC Wipe - Windows Utility

Erasing Hard Drives - Step 1



Erasing Hard Drives - Step 2

Applying Forensic Science to PCs

Must be able to prove authenticity and integrity

Evidence is what it is said to be and is not altered or contaminated in any way

Some Computer Components

BIOS
- Passwords

Operating System
- Security, bypassing

Disks
- Tracks, sectors, clusters

Disks

Deleted File only marked

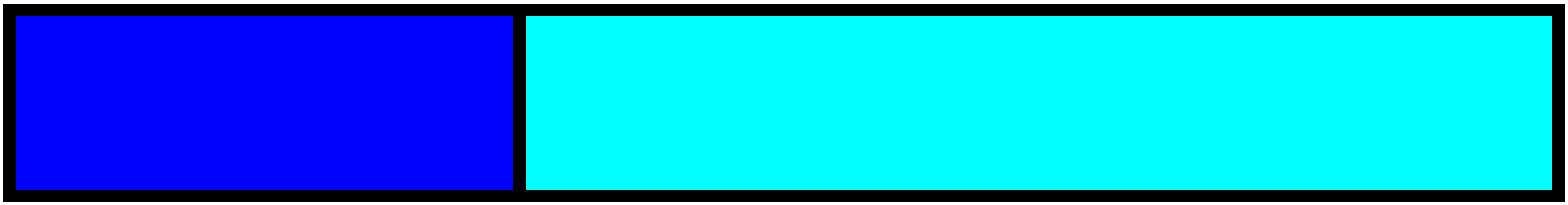
Data Still there

Overwritten files

If smaller, segments can still be there.

Slack Space

Allocated space



File Slack Space

Slack space can contain left over bits from other files.

Apply Forensic Science to Computers

Evidence can be

- Direct
- Hearsay
  - Generally inadmissable
  - Can not be cross-examine

Key Aspects

recognition

preservation, collection, document

classification, comparison, individualization

reconstruction

Recognition

Determine what devices contain digital evidence

Determine what data is relevant

Collecting and Preserving

Must be preserved in original state

Authentic and unaltered

Printouts or duplicates are admissible if the original is available for examination

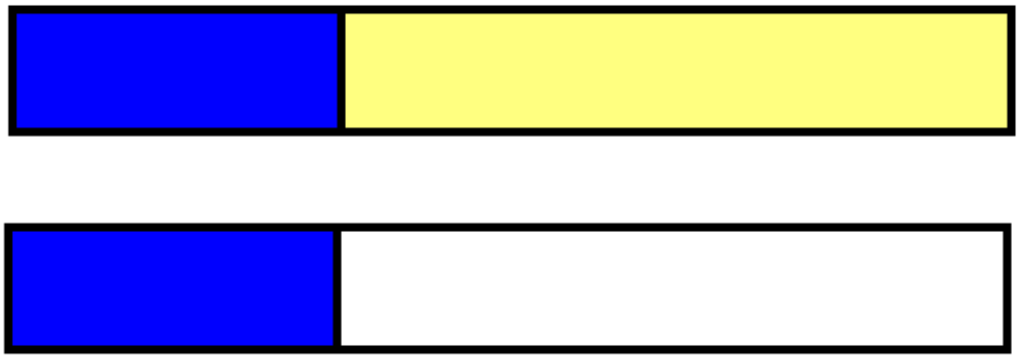
Preserving

Secure computer immediately
  If destroying data, Pull plug, not switch
  If not, save data in RAM
Write protect
Boot from another disk
Checksums (MD5)

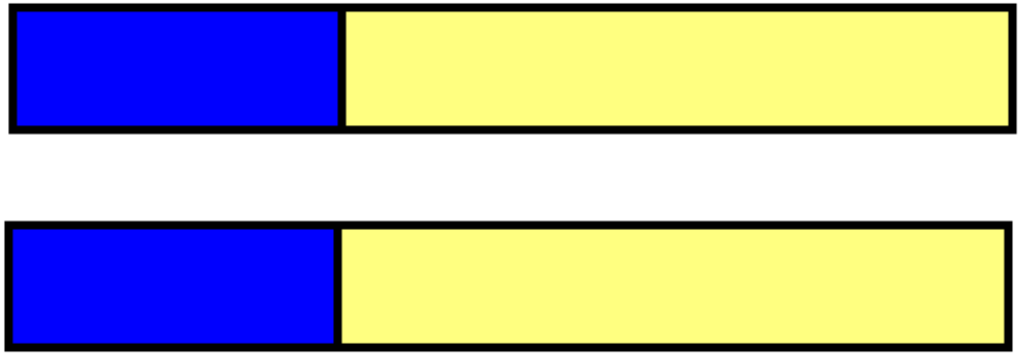
Bitstream disk copy (not file copy)
Climate control

File Copy vs. Bitstream

File Copy - Content of slack is lost



Bitstream - everything is copied



Bitstream Copy

dd

Unix Command - Disk Duplicator

Available for Windows

Create Image File from Disk

```
dd if=\\.\a: of=c:\temp\disk1.img bs=1440k
```

Create Disk From Image File

```
dd if=c:\temp\disk1.img of=\\.\a: bs=1440k
```

Things to collect

hardware
software
disks, tapes
printouts
papers
sticky notes
garbage

Empirical law of digital evidence collection and preservation

If you only make one copy of digital evidence, that evidence will be damaged or completely lost

Example: Most PCs

Get the user away
Should machine be turned off?
Save any open files to floppies
Turn off
Bypass OS (boot disk, Knoppix)
Make bitstream copy of disk
    CD-ROM, second hard disk
    Use a second machine

Documenting HW and Digital Evidence

Example: video a live chat

Labeling cables
Recording Serial Numbers
Photographs
Videotaped

Copying evidence

Label with

- Current date and time
- Initials of person who made copy
- Name of OS used
- Command used to copy
- Information believed to be in files

Message Digests

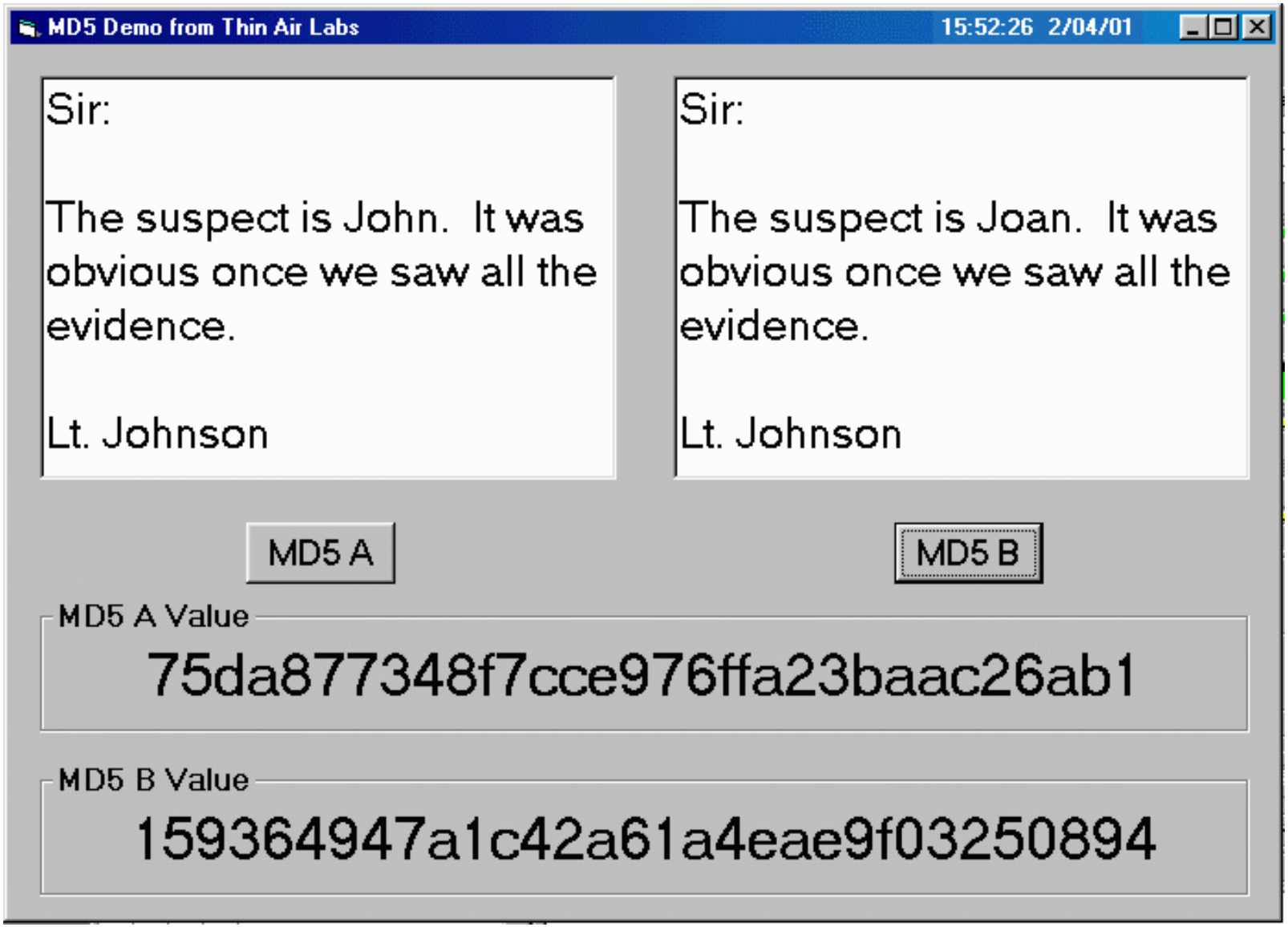
Calculates a checksum for a file

Should be unique

A single character change will alter the checksum

MD5 - generates 32 digit number

MD5 Demo


MD5 Demo from Thin Air Labs
15:52:26 2/04/01
Sir:
The suspect is John. It was obvious once we saw all the evidence.
Lt. Johnson
Sir:
The suspect is Joan. It was obvious once we saw all the evidence.
Lt. Johnson
MD5 A
MD5 B
MD5 A Value
75da877348f7cce976ffa23baac26ab1
MD5 B Value
159364947a1c42a61a4eae9f03250894

Classification, comparison and individualization of DE

Classification identifies the evidence in general terms

i.e. - email, picture, document

Comparison: Examining individual characteristics of the evidence against know items

Individualization

Linking it to a specific object

Example - Melissa Virus

MS Office embedded code
- Based on MAC Address
- Uniquely identifies the machine

Reconstruction

Rebuilding deleted, damaged, hidden or encrypted evidence.

Slack space in files
Virtual memory files
Cracking encrypted files

Reconstructing the crime

who
when
where
how
why

Case Study

Bank of Clinton

Scenario

Three customers have called the Bank of Clinton complaining that the Bank of New Hartford (a rival bank) had been soliciting their business, trying to get them to move their money over to their bank. During their solicitation the rival bank revealed information that should have been known only to the customer and the Bank of Clinton. Concerned that the Bank of Clinton was not adequately protecting their personal information, each customer quickly closed their accounts and moved their money elsewhere.

Reaction

Senior management at the Bank of Clinton were obviously very concerned with this situation. In a private meeting, management identified people that could be involved in providing information to their competitor. Jack Stewart's name continued to come up over and over.

Prime Suspect

Jack Stewart has been working as a teller at the Bank of Clinton for the last two years. Last month Jack was passed up for promotion as Teller Supervisor for a fellow employee half his age. Angry about this, Jack has since been very quiet around the work place and has been looking over his shoulder often.

The Mission

If Jack or any other BOC employee was involved, management wanted to prove it quickly and put and end to it as soon as possible. The longer this continued the more business they would lose; and their reputation could be permanently ruined.

If you decide to accept it...

You are contacted by the bank for assistance in proving the case before contacting police, and you meet with management the same day at the close of business. The bank would like you to examine a floppy disk lying on Jack Stewart's desk labeled "Customer Information".

First Steps

As a result of your instructions, no employees of the bank have touched the disk, besides Jack. You want to eliminate any change of the disk being contaminated by others viewing or accessing the contents of the disk. You have created an exact duplicate of the disk and will be performing analysis on the duplicate, so as not to alter any of the original data.

The Duplicate

forensic image: stewart-floppy.zip (filename=stewart-floppy.dd, MD5 = 6513af153d39425c88cc7a1746ffc47f)

Working with the duplicate, it appears to be a blank disk. So you start digging...

Questions

1. What did the suspect do to the disk to delete the data?

2. How did the suspect obtain the name of the president of the Bank of Hartford?

3. What is the suspect offering the president of the Bank of Hartford?

4. Were any customers of the BOC found on the floppy diskette? If so, who were they?

Questions?

End of Presentation