



# 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

The screenshot displays the WinHex application interface. On the left, a 'Details' pane shows drive information for Drive D: (7% free, NTFS, 39.1 GB total capacity). The main window is split into two panes: a file explorer view of Drive D: and a hex editor view of the selected file 'caitlin\_1.jpg'.

**File Explorer View (Drive D:)**

Filename	Size	Ext.	Created	Modified	Accessed	A...
20040315-018-x86.exe	7.5 MB	exe	3/16/2004 15:18:25	3/16/2004 15:18:40	3/16/200...	A
akenilan.exe	2.8 MB	exe	3/17/2004 09:28:54	3/17/2004 09:28:54	3/17/200...	A
aol.gif	20.3 KB	gif	7/18/2003 18:13:06	7/18/2003 18:13:07	2/4/2004 ...	A
Assignment 1 - Project Idea Paper CDN...	38.5 KB	doc	2/5/2004 13:16:14	2/5/2004 13:16:06	2/5/2004 ...	A
au.exe	1.2 MB	exe	2/18/2004 15:52:10	2/18/2004 15:52:18	3/23/200...	A
B00008CG62.01-A379EYPHA05LQM.LZ...	10.6 KB	jpg	7/11/2003 14:40:29	7/11/2003 14:40:30	3/3/2004 ...	A
Blueprints747.zip	0.8 MB	zip	3/22/2004 10:34:10	3/22/2004 10:34:18	3/25/200...	A
caitlin_1.jpg	59.1 KB	jpg	8/6/2003 08:50:33	8/6/2003 08:50:33	3/3/2004 ...	A
cg_04.jpg	43.6 KB	jpg	7/8/2003 10:14:40	7/8/2003 10:14:40	3/3/2004 ...	A
Courses in English.doc	98.5 KB	doc	1/29/2004 16:08:59	1/29/2004 16:08:59	1/29/200...	A
cover_answers.exe	16.0 KB	exe	10/10/2003 16:24:43	10/10/2003 16:24:44	3/3/2004 ...	A
cradle01.jpg	51.6 KB	jpg	7/8/2003 09:59:02	7/8/2003 09:59:02	2/4/2004 ...	A
DTAEVAL246D.exe	11.9 MB	exe	3/10/2003 11:01:32	3/10/2003 11:01:34	6/5/2003 ...	A
erarc201.zip	54.0 KB	zip	9/24/2003 15:26:35	9/24/2003 15:26:30	9/24/200...	A
excel-password-recovery.exe	0.6 MB	exe	3/11/2004 11:45:45	3/11/2004 11:45:52	3/11/200...	A
foundstone_tools.zip	4.7 MB	zip	6/23/2003 08:28:51	6/23/2003 08:28:52	2/18/200...	A
getrt500.exe	2.3 MB	exe	5/5/2003 09:54:03	5/5/2003 09:54:04	6/5/2003 ...	A
Gleason.doc	32.0 KB	doc	12/15/2003 15:17:09	12/15/2003 15:17:09	12/15/20...	A
imailsrv2.zip	51.5 KB	zip	2/4/2004 15:24:57	2/4/2004 15:24:58	3/3/2004 ...	A

**Hex Editor View (caitlin\_1.jpg)**

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Access
96DC30000	EF	D8	FF	E0	00	10	4A	46	49	46	00	01	02	00	00	64	ÿ@ÿà...JFIF.....d
96DC30010	00	64	00	00	FF	EC	00	11	44	75	63	6B	79	00	01	00	.d..ÿi...Ducky...
96DC30020	04	00	00	00	49	00	00	FF	E2	0C	58	49	43	43	5F	50	....I..ÿà.XICC_P
96DC30030	52	4F	46	49	4C	45	00	01	01	00	00	0C	48	4C	69	6E	ROFILE.....HLin
96DC30040	6F	02	10	00	00	6D	6E	74	72	52	47	42	20	58	59	5A	o.
96DC30050	20	07	CE	00	02	00	09	00	06	00	31	00	00	61	63	73	o.
96DC30060	70	4D	53	46	54	00	00	00	00	49	45	43	20	73	52	47	pM
96DC30070	42	00	00	00	00	00	00	00	00	00	00	00	01	00	00	F6	B.
96DC30080	D6	00	01	00	00	00	00	D3	2D	48	50	20	20	00	00	00	Ö.
96DC30090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
96DC300A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
96DC300B0	00	00	00	00	00	00	00	00	00	00	00	00	11	63	70	72	.....cpr
96DC300C0	74	00	00	01	50	00	00	00	33	64	65	73	63	00	00	01	t...P...3desc...
96DC300D0	84	00	00	00	6C	77	74	70	74	00	00	01	F0	00	00	00	█...lwtpt...ÿ...
96DC300E0	14	62	6B	70	74	00	00	02	04	00	00	00	14	72	58	59	.bkpt.....rXY
96DC300F0	5A	00	00	02	18	00	00	00	14	67	58	59	5A	00	00	02	Z.....gXYZ...

**Data Interpreter**

- 8 Bit (±): -1
- 16 Bit (±): -9985
- 32 Bit (±): -520103681

**Status Bar:** Sector 79094144 of 81915368 | Offset: 96DC30000 | = 255 | Block: n/a | Size: n/a

# 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.

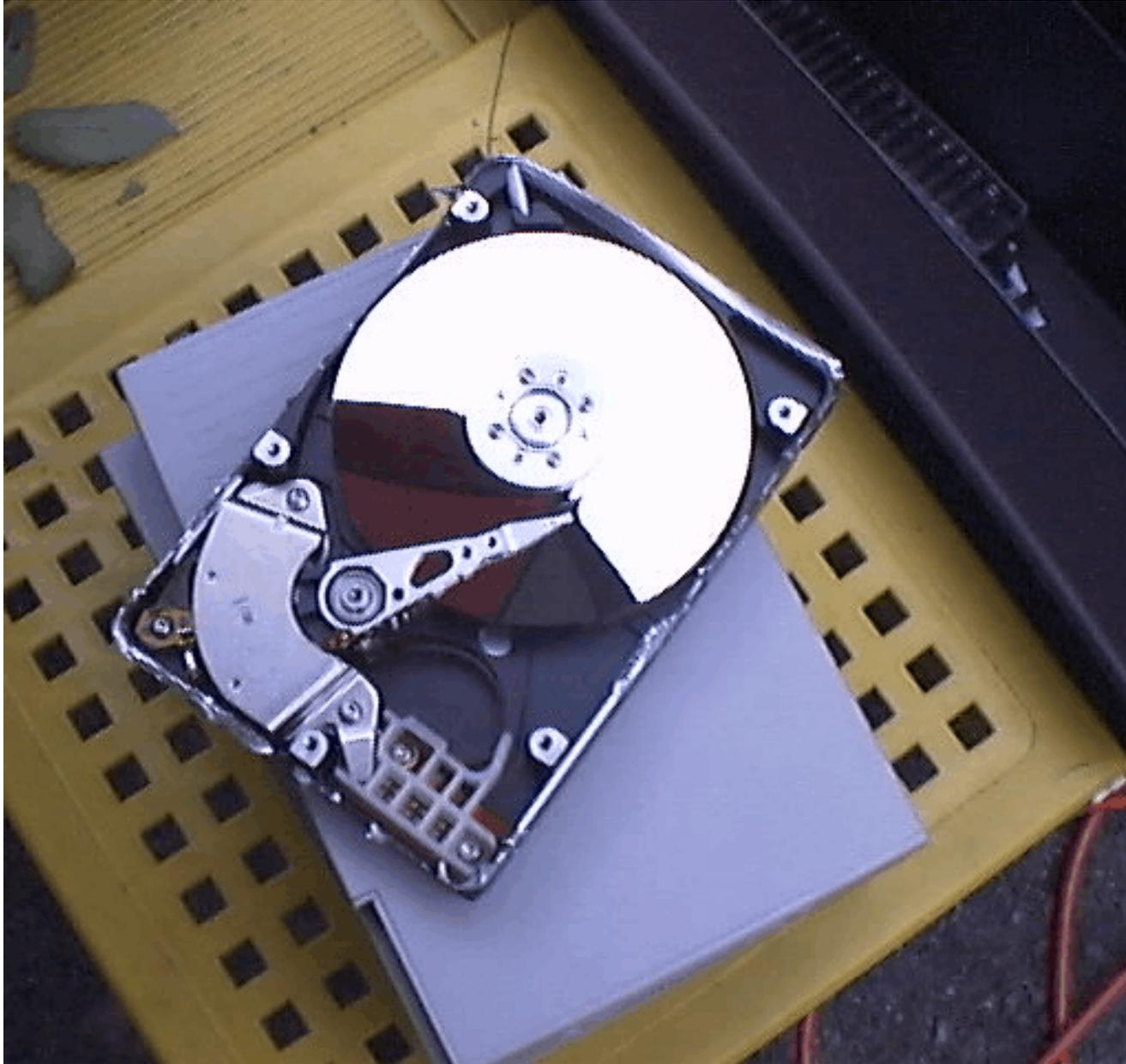
Delete Files

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

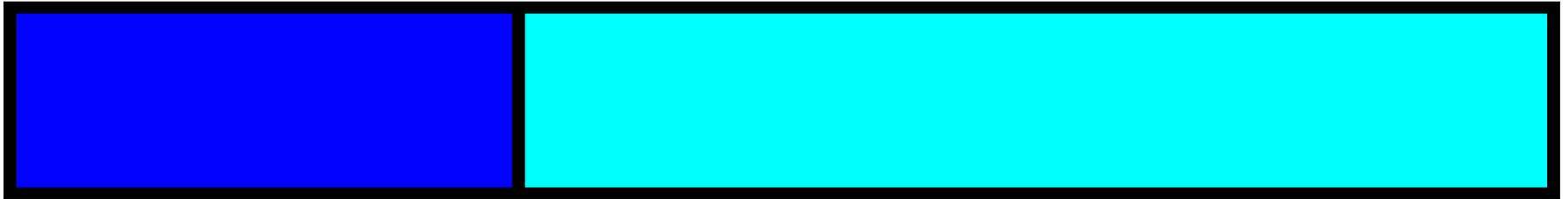
Deleted File only marked  
Data Still there

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 inadmissible

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)

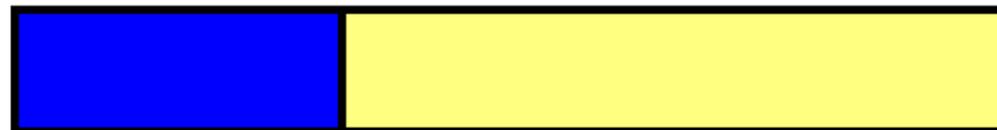
Climate control

# 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

The screenshot shows a window titled "MD5 Demo from Thin Air Labs" with a timestamp of "15:52:26 2/04/01". The window is divided into two columns. Each column contains a text input field with the text "Sir:" followed by "The suspect is John. It was obvious once we saw all the evidence." and "Lt. Johnson". Below each text input is a button labeled "MD5 A" and "MD5 B" respectively. Below the buttons are two large text boxes displaying the MD5 hash values for each input.

Input Text	MD5 Hash Value
Sir: The suspect is John. It was obvious once we saw all the evidence. Lt. Johnson	75da877348f7cce976ffa23baac26ab1
Sir: The suspect is Joan. It was obvious once we saw all the evidence. Lt. Johnson	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 an 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**