

# Computer Forensics

Anna Suen  
January 30, 2002

1

## Outline

- Definition of computer forensics
- Sample Scenario
- Computer Evidence
- Gathering the Evidence

2

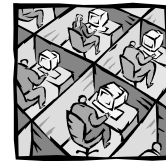
## What Is Computer Forensics?

- gathering of computer evidence
- using this evidence in legal proceedings

3

*Typical employee misconduct scenario....*

Mark is one of four happy system administrators at a local medium-sized financial firm called Jay Mars Financials.



4

One day, Mark receives a message from his boss that his position has been removed due to corporate downsizing and restructuring.



Mark is very angry at the situation. He still has a family with a wife, two kids, a dog, and a parrot to feed.



Mark decides to take revenge....

5

Mark writes a simple program, set to execute the night after his last day, to corrupt one of the firm's databases and back up the corrupted data.



Mark wrote the program from his PC at home and ftp-ed it over to the firm's server. And then deleted the program off of his computer.

6

At the designated time, the program executes. Essential client data is lost. The firm tries to restore the data, but the backup is also corrupted.



This causes Jay Mars Financials to suffer significant financial loss, harming the company's hard-won reputation.



7

Jay Mars Financials immediately starts investigating the situation. They call in computer forensics specialists, who identify Mark as the main suspect.



Mark's personal computer is seized and forensically analyzed. They recover the actual program code! This code is preserved as computer evidence.

*To be continued....* 8

## Computer Evidence

- 3 types:
  - open data
  - unknown or potentially unknown data
  - hidden data

9

## Computer Evidence: Open Data

- operating system:
  - executables
  - configuration files
  - temporary files
- user application software
  - configuration
  - data
  - work files
- user generated data

10

## Computer Evidence: Unknown/Potentially Unknown Data

- ambient computer data
  - Windows swap file
  - file slack
    - residual data
  - unallocated file space

11

## Computer Evidence: Hidden Data

- encrypted data
- partition waste space
- bad sectors
- extra tracks
- disguising data
- steganography

12

## Gathering the Evidence

- Tools:
  - dedicated machines
  - software
- Preservation
  - proper training
  - copy of the evidence
- Good methodology
- Take legal action

13

*Continuing with our scenario....*

Jay Mars Financials took legal action against Mark. Mark is ordered to pay for the damages and is put in jail.



THE END.

14

## Ideas For My DIS Paper

- Database forensics:
  - How to perform forensics on databases?
  - How is forensics different for databases (if at all)?
- Any other ideas?

15