Computer Forensics: Hiding in Plain Sight

Dr. Kara L. Nance
ASSERT Center
University of Alaska Fairbanks

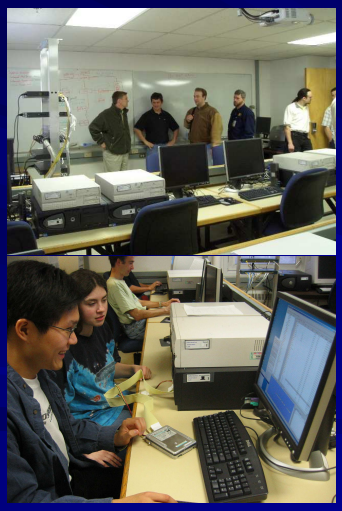
Overview

- Introduction
  - University of Alaska
  - ASSERT Center
  - ASSERT Lab
- Computer Forensics
- Disk Forensics
  - BTK Killer
  - File Metadata
  - Data Recovery
- Redaction
- Steganography

University of Alaska – Computer Science

- ABET Accredited Computer Science Program.
- B.S., M.S., M.S.E.
- Diverse faculty research expertise with emphasis on
  - Information Assurance
  - Computer Graphics

Advanced System Security Education, Research, and Training (ASSERT) Lab



- Computer Forensics
- Information Assurance
- Computer Security
- Authentication
- Networks
- Honeypots
- Virus and Worm Behavior
- Social Engineering
- Critical Infrastructure
- Sensor Webs
- Education/Outreach

www.assert.uaf.edu

Computer Security

"We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable - to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."

National Research Council, "Computers at Risk" National Academy Press, 1991.

Computer Forensics

[T]he application of computer investigation and analysis techniques to gather evidence suitable for presentation in a court of law.

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1007675,00.html

Computer Forensics

- Disk Forensics
- Network Forensics
- Corporate Forensics

The BTK Killer

- In January 1974, murdered the Otero family, including two children ages 9 and 11.
- In April 1974, killed a 21-year-old woman.
- In 1977, strangled a woman in front of her children.
- December 1977, strangled a woman and reported the murder himself.
- Sent numerous letters and clues to police.
- Continued killing and sending letters, tokens, and clues from past crimes.

http://www.cbsnews.com/stories/2005/09/29/48hours/main890980.shtml

The BTK Killer

"[H]e sent a note asking whether he could send police a computer disk and still stay anonymous. He wrote,

"Look, be honest with me. If I send you a disk will it be traceable? Just put [the answer] in the newspaper."

BTK even suggested a secret code number for the communication."

http://www.cbsnews.com/stories/2005/09/29/48hours/main890980.shtml

The BTK Killer

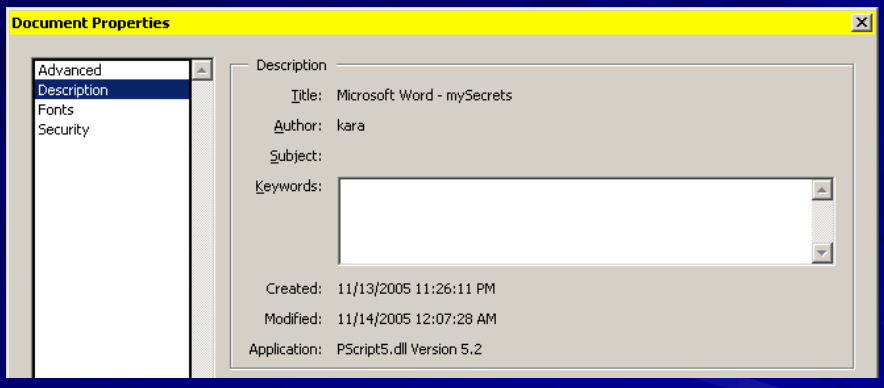
- "It was the break that the police needed. They placed a coded ad in the newspaper, following BTK's instructions. Assured of anonymity, BTK sent in a disk. And he was trapped."
- "It took no time for computer experts to trace the disk to a local church, and a user named Dennis. A Google search turned up a Dennis Rader, president of the Christ Lutheran Church."

http://www.cbsnews.com/stories/2005/09/29/48hours/main890980.shtml

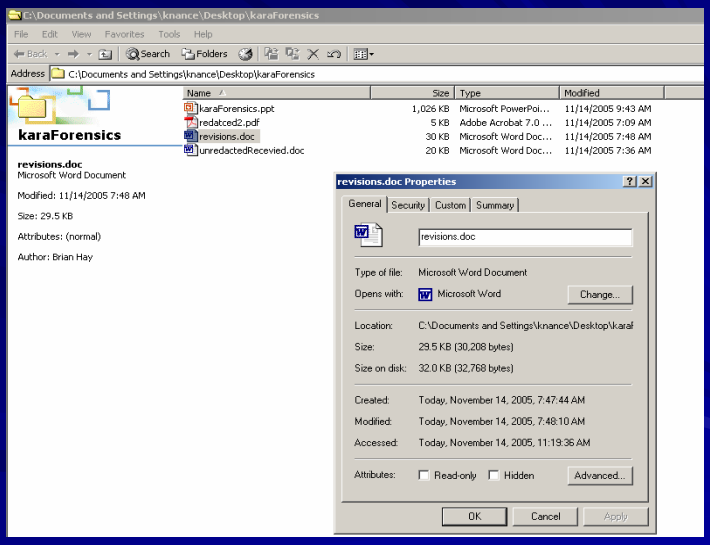
File Metadata

- The operating system typically records information about the creation and modification dates of files.
- Modern data files (e.g. Microsoft Office, PDF, etc.) also often contain considerable amounts of metadata, including:
  - File author
  - Creation Time
  - Last Modification Time
  - Software Version

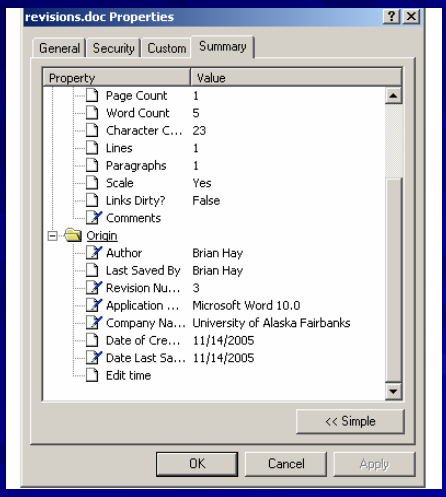
File Metadata



File Metadata

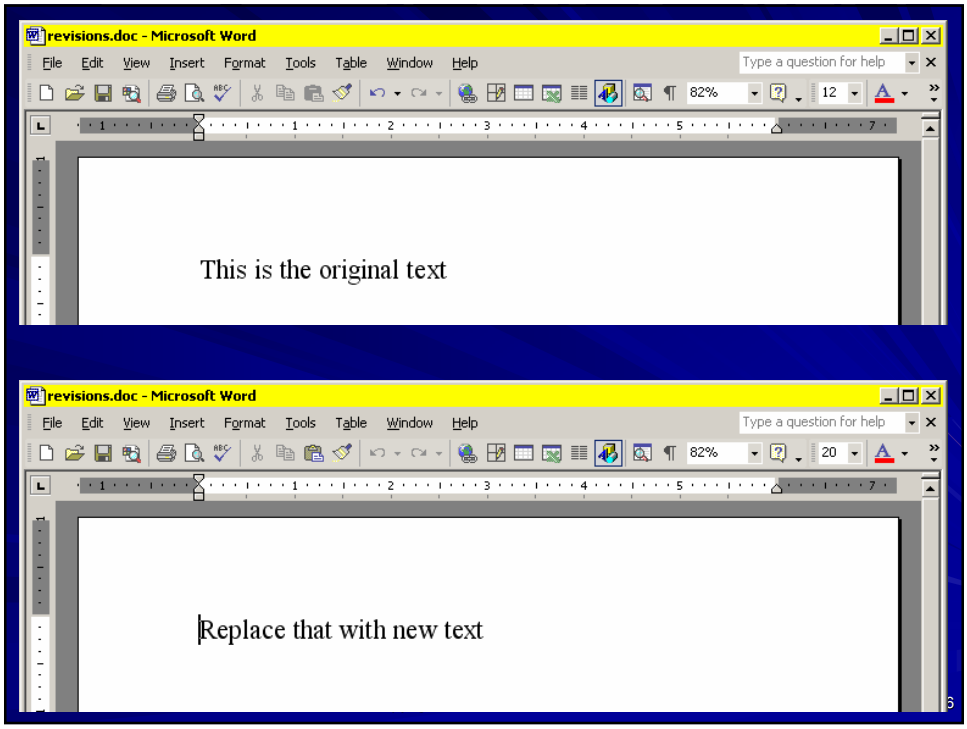


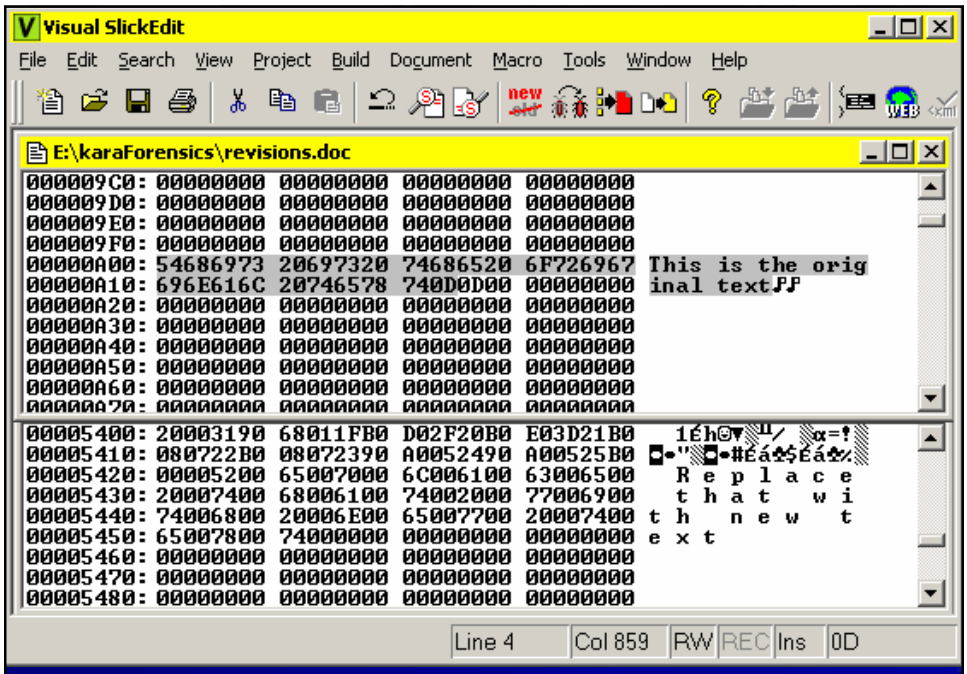
File Metadata



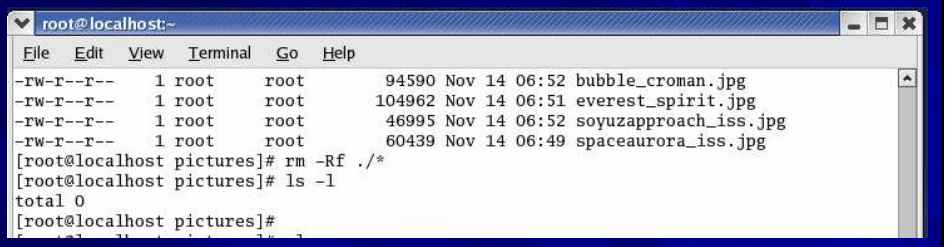
Revision History

- In some cases, deleting data from a document may not actually delete the data from the file.
- While the old version may not be visible, it may be possible to recover it.



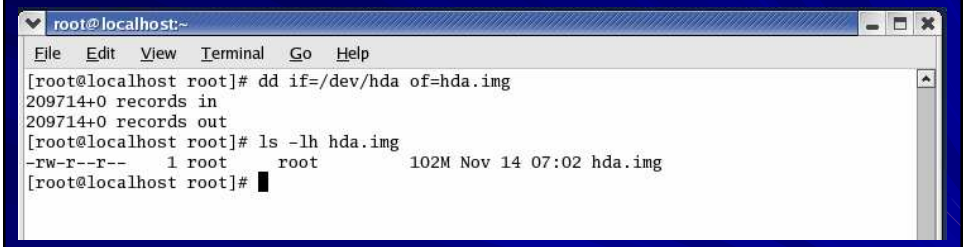


Data Recovery



- Four pictures are accidentally deleted from a disk.
- Data recovery may be possible, depending on what occurs between deletion and recovery.

Data Recovery



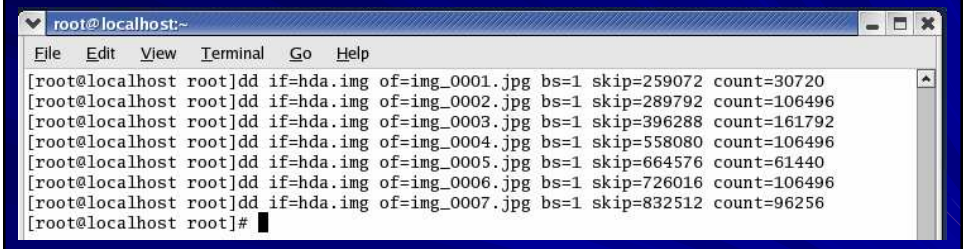
- An image of the disk is made, which can then be used for data recovery without jeopardizing the original data.

Data Recovery

```
000CB3F0: 00000000 00000000 00000000 00000000 ................
000CB400: FFD8FFE0 00104A46 49460001 02000064 ......JFIF.....d
000CB410: 00640000 FFFE0012 41646F62 6520496D .d......Adobe Im
000CB420: 61676552 65616479 FFEC0011 4475636B ageReady....Duck
000CB430: 79000100 04000000 3C0000FF EE000E41 y.......<.......A
000CB440: 646F6265 0064C000 000001FF DB008400 dobe.d..........
000CB450: 06040404 05040605 05060906 0506090B ..........□. . □.
000CB460: 08060608 0B0C0A0A 0B0A0A0C 100C0C0C ......□□.□□.....
```

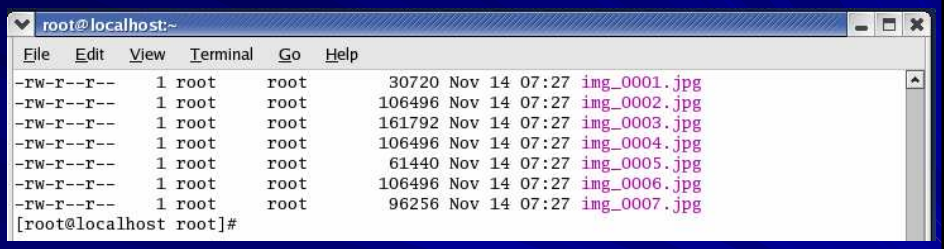
- JPEG files start with a known *byte sequence*, so we can quickly determine where each JPEG file starts, and then recover the entire file from that point.

Data Recovery



- Once the start location of each file is known, *dd* can be used to copy a section of the data from that location to a new file.

Data Recovery



- Seven images are recovered in this case, which include the four images recently deleted, and three other images that had been previously stored on the disk.

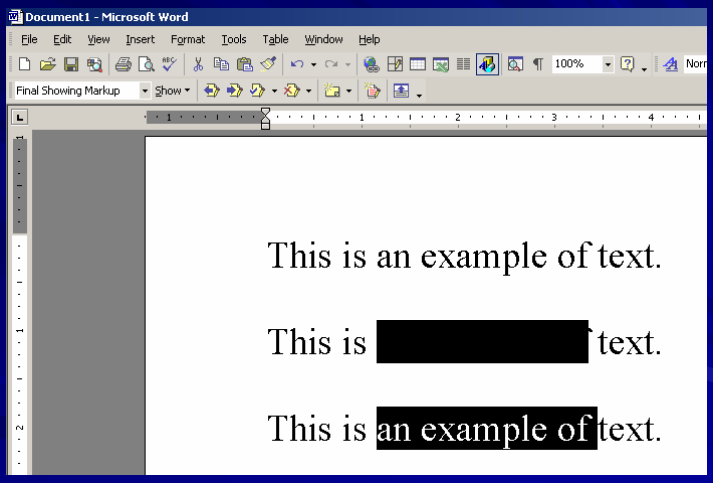
Recovered image, originally obtained from
http://antwrp.gsfc.nasa.gov/apod/image/0511/spaceaurora_iss.jpg

Redaction

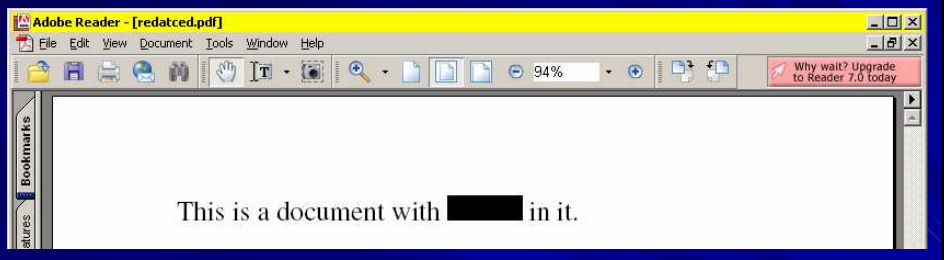
This is [redacted] going to be the most [redacted] part of this [redacted] and [redacted] talk.

- Redaction involves the removal of “sensitive” information from a document.
- Important in many domains, including government, military, legal, education, etc.

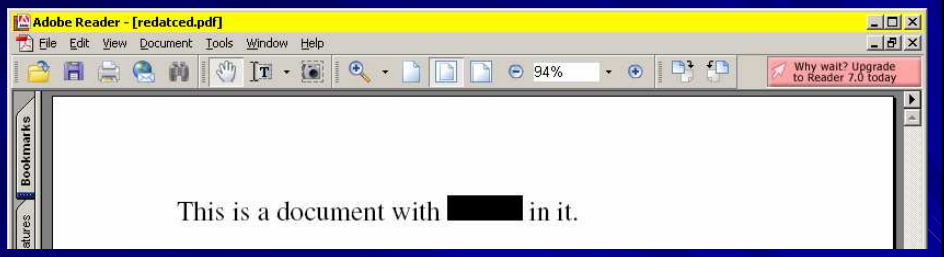
Redaction Example



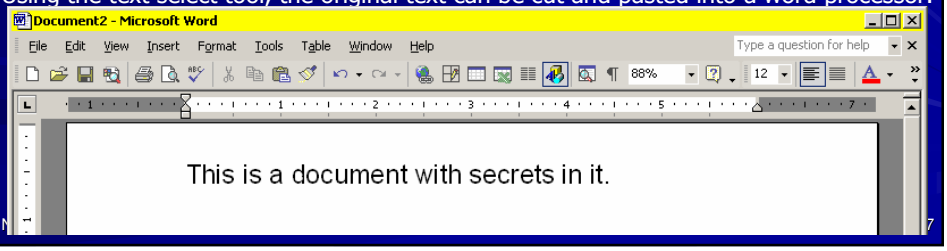
Redaction Example



Redaction Example



Using the text select tool, the original text can be cut and pasted into a word processor.



Redaction Example

- Redaction tools are now available that (hopefully) perform this task more effectively.
  - MS Office 2003 Word Redaction Add-in
  - Redax (PDF document redaction).

**Some works suggest that some redacted data can still be recovered if black bars are placed over words by examining the characteristics of the bar used.

Steganography

*[T]*he science of *hiding* information.

Whereas the goal of cryptography is to make data unreadable by a third party, the goal of steganography is to hide the data from a third party.

http://www.garykessler.net/library/steganography.html

Steganography Example

- Write with white font on a white background in a document or on a web page.
- Embed text in an image.
- Hidden functions in web page.

Steganography

- 10010101 00001101 11001001 10010110 00001111 11001010 10011111 00010000 …
- Suppose I want to “hide” a message “hello” in the image.
- h - 01101000
- If we overlay these 9 bits over the least significant bits of the 8 bytes above, we get the following (where bits in red have been changed):
- 10010100 00001101 11001001 10010110 00001111 11001010 10011111 00010000 …

Steganography Example

S-tools

available from

http://www.webattack.com/download/dlstools.shtml)

Questions?

This presentation is available at the ASSERT Center website

http://assert.uaf.edu