DHS-ICE Computer Forensics

Special Agent Scott Lowen
DHS/ICE Miami, Florida

COMPUTER/DIGITAL FORENSICS DEFINED

The process of:

1) Identifying,
2) Collecting,
3) Preserving,
4) Analyzing,
5) Documenting,

facts about digital evidence.

(Computers are only one source of digital evidence.)

THE VALUE OF COMPUTER FORENSICS

- Verification of facts
  - Emails
  - Documents
  - Time frames
  - Pictures
- Data Recovery
  - Lost or deleted files/systems

WHEN DO YOU NEED COMPUTER FORENSICS?

Criminal Activity

Civil Proceedings

Administrative Actions

Capabilities

- Reveals direct evidence on the machine
- Associates a machine with data
- Provides investigative leads
- Reveals evidence that corroborates or refutes allegations or alibis
- Reveals behavioral evidence

Case Agent-Examiner Relationship

- The case agent and forensic examiner must work as a team
- Case agent
  - Involves examiner early
  - Explains case
  - Provides focused requests
- Forensic examiner
  - Educates and advises investigator
  - Explains results and limitations

Introduction

computer forensics

- In 1998 only a few cases involved seizing computers. Now almost every case involves a seized computer.
- The explosion of the Internet has created a whole new arena for the facilitation of crime.
- Technology constantly changing causing computer forensics to change and adapt.

Computer Forensic Challenges

- Bigger
  - The largest hard drive in 1998 was 9 GB today it is 2 TB.
- Cheaper
  - The 9 GB hard drive from 1998 cost $1,500 and the 2TB drive of today costs $200
- Smaller
  - xD cards, SD cards, Mini and Micro SD cards, and thumb drives offer small cheap concealable storage devices.

DATA CONSIDERATIONS

- **Timeliness (GET THE DATA ASAP)**
- **Volume**
  - **Bit, Byte, Kilobyte, Megabyte, Gigabyte, Terabyte, Petabyte**
  - **1 page (Word document) = 25Kb.**
  - **40 pages (Word documents) = 1 Mb.**
  - **40,000 pages= 1 Gb.**
  - **4,000,000 pages = 100 Gb. (1,333')**
- **Storage of Duplicate Digital Evidence (DDE)**

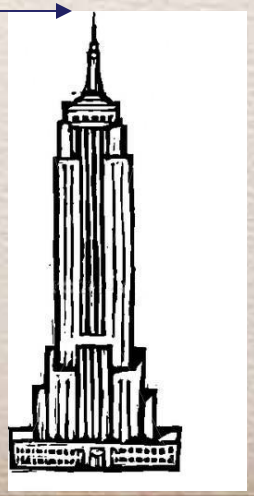
Forensic Exams Challenges

4000 feet

- A 80 GB Hard Drive can hold the text in a stack of documents approximately 4000 feet high.

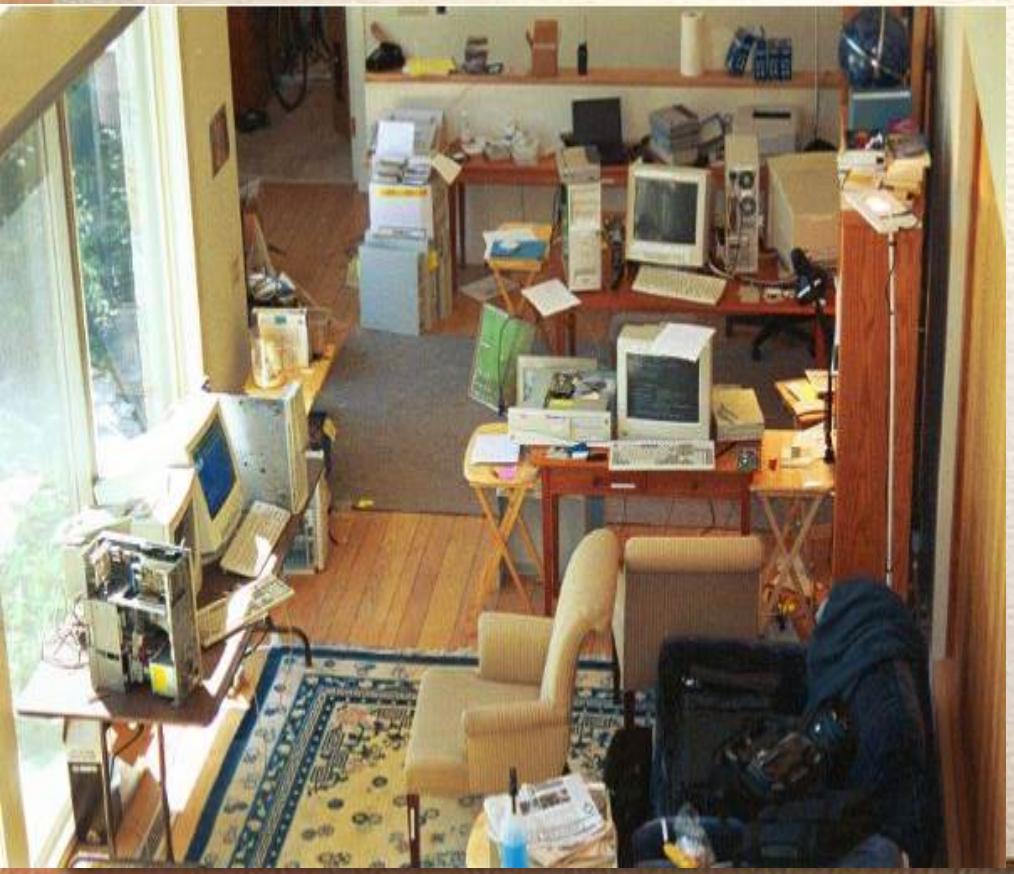
computer forensics

Empire State Building – 1454 feet



- In FY-2007 DHS-ICE Computer Forensic Agents (CFAs) conducted 3,940 computer forensic examinations encompassing approximately 278 TB of data.
- Since the inception of the Computer Forensic Program in 1997, Customs/ICE Computer Forensic Agents have completed 15,901 computer forensic examinations.
- The number of examinations completed has nearly doubled every year since 1997. This trend is expected to continue into the future.

A Bad Day In The Life Of A CFA



Theory of Stupidity

- As law enforcement officers we like to say that we only catch the dumb criminals.
- If we caught the smart ones we would have no more crime.
- This is certainly true will all aspects of law enforcement including cyber investigations.
- Those using complex encryption and sophisticated IP spoofing are generally not the cyber criminals caught by law enforcement.

Forensic Dilemma

- The computer forensic process relies on making an exact image copy of all suspect digital evidence and then performing an analysis using the copy leaving the original unaltered.
- This means we need to capture both allocated and unallocated data.
- As storage capacities of hard drives explode we as computer forensic examiners must find ever increasing means of archiving seized data.

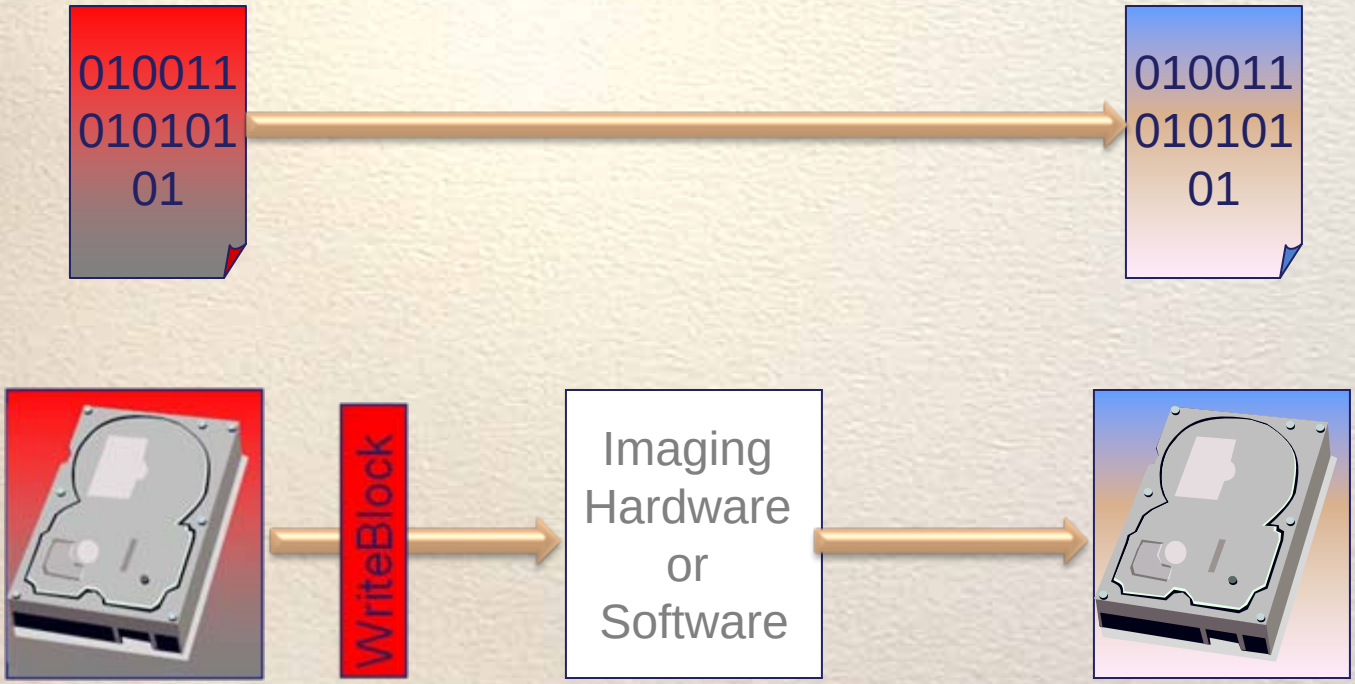
Computer Forensic Process

- The computer forensic process involves obtaining a bit image copy of a suspect computer system or other computer based media. All subsequent analysis is performed utilizing the copy. This is commonly referred to as the “Safety Net Procedure”.

Basic Imaging Methodology

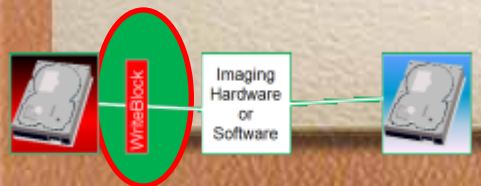
- Hard drives are generally removed from the suspect system and connected to a lab computer and imaged in a Windows environment.
- The forensic analysis is done with all inclusive tools such as Encase, or FTK.

The Imaging Process

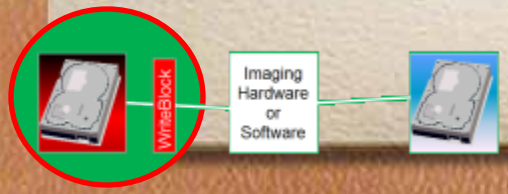


Physical Write Blocks

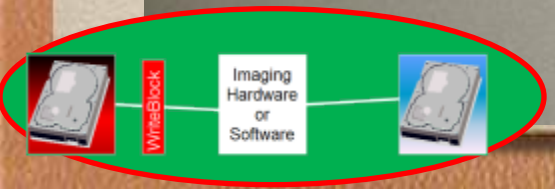
- What Are They?
  - Physical device that prevents writes to the evidence drive
  - BEST method of imaging



Attaching Write Block



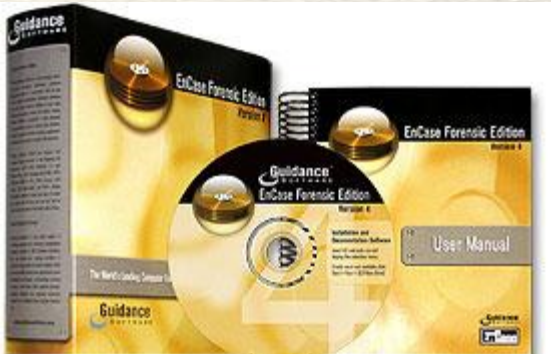
Attaching Write Block



Hardware Imager

Software Imaging

- Bootable CDs or floppies
- Control computer so it only issues read commands to the drive, never write
- Examples:
  - FTK Imager
  - EnCase



SafeBack 3.0
Evidence Grade Bitstream Backup Utility

Hard Drive Storage Problems

- Dramatically increase to time it takes to acquire and image of a suspect drive.
- Causes severe problems with archiving suspect hard drive images.
- Severely hinders the investigators ability to search the computer evidence.
- Greatly increases the time it takes to complete a computer forensic analysis.

Final Note On Hard Drive Storage

- Seven years ago, searching a computer was compared to searching a filing cabinet full of documents. It was possible to look at every file on the suspect computer. Now, searching a computer is like searching a large house. We look in all the usual hiding places based on the investigative information, but we may not find everything that may be relevant to the investigation. It is likely that an analysis done by two different investigators may not yield the exact same results.

What Can the Examiner Find?

- Deleted files
- Text fragments
- Enhanced metafiles (previously printed files)
- **Financial files (Quicken, Turbo Tax)**
- Date/time stamp information
- E-mail messages and chat logs
- Internet usage information (history)
- E-mail attachments
- Images (active and deleted)
- **Multimedia**

- AND MORE...

Forensic Request from Case Agent

- EXAMPLE: Kidnapping assault of Heather Miller
  - Evidence of defendant's involvement with abduction
  - Search for victim's name
  - Pictures of victim
  - Evidence of threatening letter sent to victim
  - Evidence of references to date rape drugs
  - Evidence of conspirator
  - Activity on the computer during time of crime

Types of Email Metadata

- What types of Metadata are available
  - When Created
  - How Created
  - When Sent
  - When Received
  - Who Sent/Received
  - Route
  - Time Analysis
  - Graphic Analysis
    - Origination
    - Who Created it
    - When Created

Things In Our Favor

- Suspects are generally “low-tech” users.
- Suspects hopefully don’t know that we are coming to seize their computer.
- Most suspects involved in computer related crimes are not hardened criminals and will generally cooperate when faced with overwhelming evidence and the possibility of incarceration.

Problems in Computer Forensics

- A new field of study
- No standardized certification
- No standardized training
- No standardized procedures
- Technology changes rapidly

Forensic Exams

computer forensics

What Can Computer Forensics Do For You Now?

- At this point not much.
- There are a few facilities around the country that may be able to recover some data.

Forensic Exams Analysis

computer forensics

- Key points to performing a computer forensic analysis:
  - Determine if the suspect digital media contains evidence of the crime being investigated.
  - Determine the source of the evidence.
  - Establish knowledge of the evidence on behalf of the computer user.
- Use information provided by the Case Agent to narrow search for evidentiary data.
  - Keyword searches

Forensic Exams Analysis

computer forensics

- Can take several weeks to complete depending on the volume of data and the case complexity.
- CFA maybe working on more than one exam at a time

Final Note

- Computer forensics is here to stay. In 1998 only a few cases involved seizing computers. Now almost every case involves a seized computer.
- The explosion of the Internet has created a whole new arena for crime.
- The computer forensic environment is constantly changing to meet the demands of technology

Summary

- Electronic evidence is everywhere
- Case agents must work closely with examiners
- Forensic examiners must look beyond the “Single File”
- Metadata can be critical to establishing user attribution
- Even if evidence itself has been deleted/destroyed, numerous artifacts can be found

QUESTIONS???

Scott Lowen

DHS/ICE, SAC Miami

11226 N.W. 20 Street

Miami, Florida 33172

305-597-6000 Office