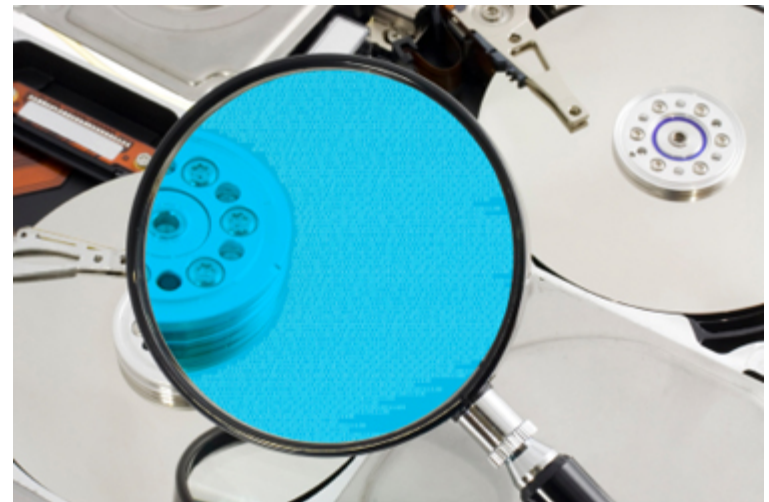
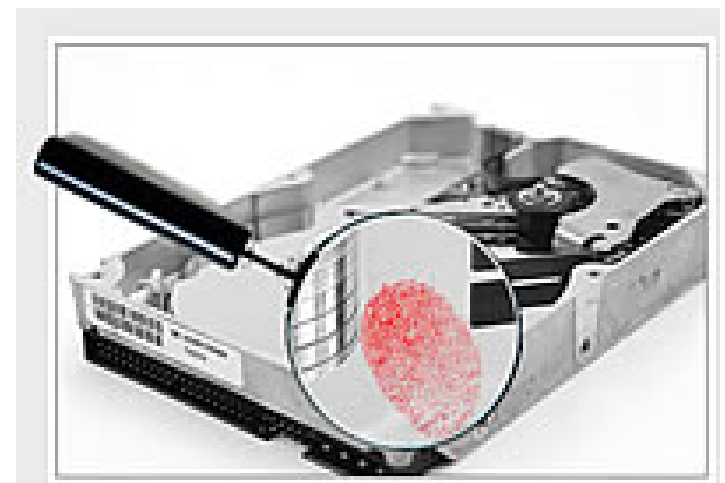


Overview

- Introduction
- Assessing the Case
- Taking a Systematic Approach
- Securing the Evidence
- Employee Termination Investigations
- Media Leak Investigations
- Industrial Espionage Investigations



(Note: you are expected to read all the links in this presentations that related to specific cases/ examples - many of them are as recent as from Oct 2009)

Introduction

- Computer Forensics: investigates data that can be retrieved from a computer's hard disk or other storage media

- Computer forensics investigators:
 - retrieve information from the computer and/ or its component parts
 - information retrieved may already be on the disk – but not easy to find or recover

- Network Forensics: yields information about how a perpetrator or an attacker gained access to a network

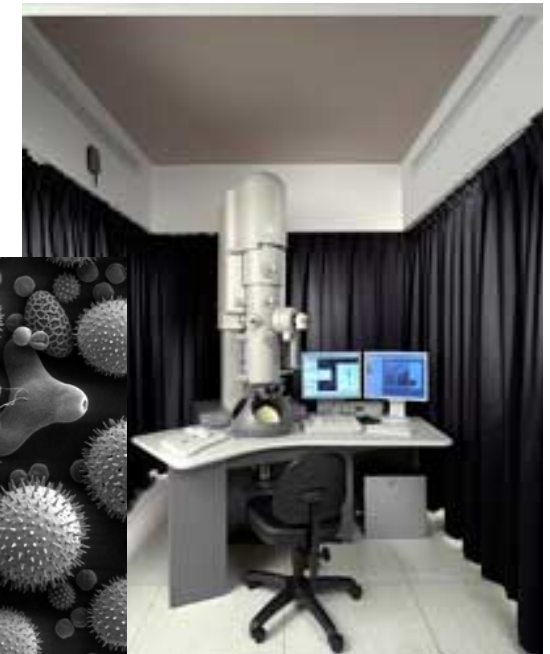
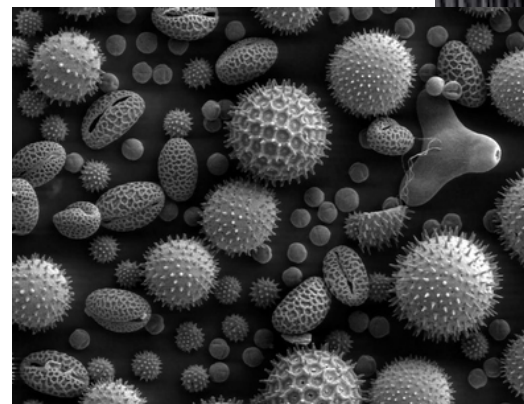
- Network forensics investigators:
 - use log files to determine when users logged on, frequency, URLs visited and for how long, how they logged on, from what location etc.

Introduction

- Computer/ Network forensics specialists may be the same person or each part of the investigative group
- Hot career – why?
- Richard Heene and the Balloon Boy Saga
- Child Pornography:
<http://www.chron.com/disp/story.mpl/metropolitan/6690367.html>
- Civil Litigation
[http://www.reuters.com/article/pressRelease/idUS182125+26-Oct-2009+BW20091026\](http://www.reuters.com/article/pressRelease/idUS182125+26-Oct-2009+BW20091026)
- Anna Nicole Smith
http://www.enewscourier.com/entertainment/local_story_299095231.html

Introduction

- How is **computer forensics** is different from normal data recovery?
- In forensics, the 'recovery' of data must be carried out in such a way that can be used as admissible evidence in court. This evidence can either be:
 - Inculpatory or
 - Exculpatory
- Various software and tools
 - e.g. EnCase, ProDiscovery
 - electron microscope (\$3,000 – 20,000)



Brief History

- Relatively new field
- Currently: computers are the **instruments** and the **targets** of many crimes
- 1970's:
 - electronic crimes – mainframe
 - computer users were experts and only certain industries used computers
 - White-collared fraud – banking industry
 - One half-cent crime

Brief History

- 1970's:
 - The Federal Rules of Evidence controlled the use of digital evidence

- 1984:
 - Due to increasing number of cases involving digital evidence, the Computer Analysis and Response Team (CART) was formed

- Late 1990's:
 - CART teamed up with DOD's Computer Forensics Laboratory (DCFI)
 - The International Association of Computer Investigative Specialists (IACIS) introduced training in software for forensics investigations

Examples of Crimes Solved Using Forensics

Criminal	Type of Crime	Type of E-Evidence
Dennis Rader	Serial killer	Deleted files on a floppy disk used by the criminal at his church's computer
Lee Boyd Malvo, John Allen Muhammad	Snipers	Digital recordings on a device in suspects' car
Lisa Montgomery	Murder and fetus-kidnapping	E-mail communication between the victim and criminal—tracing an IP address to a computer at criminal's home

Let's not forget one of the most famous corporate cases that has involved a substantial amount of computer forensics

Crimes Solved Using Forensics (Cont.)

Criminal	Type of Crime	Type of E-Evidence
David A. Westerfield	Murder	Files on four computer hard drives and a PDA
Scott Peterson	Double murder	GPS data from his car and cell phone; Internet history
Alejandro Avila	Rape and murder	E-evidence of child pornography on his computer
Zacarias Moussaoui	Terrorism	E-mail, files from his computers

Recent gang rape case ...review of Facebook and YouTube..

http://www.nydailynews.com/news/national/2009/10/27/2009-10-27_richmond_high_school_gang_rape_cops_arrest_2_in_attack_on_calif_teen_girl_bystan.html

Forensics Investigation Methods

- Methods used by investigators must achieve many of these objectives:
 - Protect the suspect system
 - Discover all files (text/ video/ audio/ pictures/ emails etc.)
 - Recover deleted files
 - Reveal contents of hidden files
 - Access protected or encrypted files
 - Use steganalysis to identify hidden data
 - Analyze data in unallocated and slack space
 - Print an analysis of the system
 - Provide an opinion of the system layout
 - Provide expert testimony or consultation

Examples of Tools and Resources

- Software:
 - iLook
 - EnCase
 - ProDiscovery
 - AccessData Forensic Toolkit (FTK)

- Trade Publications:
 - Forensics Magazine: <http://www.forensicmag.com/articles.asp?pid=138>
 - Computer Forensics Magazine

- Groups/ Forums:
 - Computer Technology Investigators Network (CTIN)

- Associations:
 - High Technology Crime Investigation Association (HTCIA)

Assessing the Case

- Imagine that you are the Computer Forensics Specialist... Before you start, there are some things to consider
- Situation: corporate employee abuse case, pornography, murder/ homicide/ suicide ...
- Types of evidence:
- Operating Systems:
- Locations of evidence
- Descriptions of evidence
- antistatic bags, tapes, tags, labels and _____

First Responder Seizure Record		
---------------------------------------	--	--

Fill in one form per item seized

Case No.		/		Case Name	
Location of Seizure					
Full Address:	Room No				
	Building				
	Address Line 1				
	Address Line 2				
	Address Line 3				
Address Line 4	Post code				
Details of Evidence Seized					
Type: (E.g. computer, disk, paper etc)				Where Located	
Make				Model	
Serial No:				Evidence Bag No:	
Acquisition Details					
Have you enquired of the owner any passwords used?				YES	NO
<i>If yes to above please state passwords and how used.</i>					
Was the equipment attached to a telephone line at the time of seizure?				YES	NO
Was the equipment switched on at the time of seizure?				YES	NO
<i>If yes to above please state how equipment was switched off and secured.</i>					
Has the equipment been switched on since being seized?				YES	NO
<i>If yes to above please state the reason and the details of the person.</i>					
Photos of exhibit taken (if so attach them)	YES	NO	Sketch produced (if so attach it)	YES	NO
Witness Signature (Forensic Analyst making seizure)					
Full Name:				Title:	
Phone:				Department:	
Signature:				Date and time:	
Witness Signature (Second signature only if required)					
Full Name:				Title:	
Phone:				Department:	
Signature:				Date and time:	

Typical Nature of Corporate Cases

- Forensics experts are called in for several types of cases. Some such examples are:
 - Employee Termination Cases
 - Media Leak Investigations
 - Industrial Espionage Investigations

Employee Termination Cases

- Majority of these involve the abuse of corporate assets
- Also predominant are contributing to hostile work environment
 - Distributing emails/ pictures that are offensive - e.g. _____
 - Examples at Brooklyn and MU
- 2 main types of Investigations:
 - Internet Abuse
 - Email/ IM/ text abuse

Employee Termination Cases

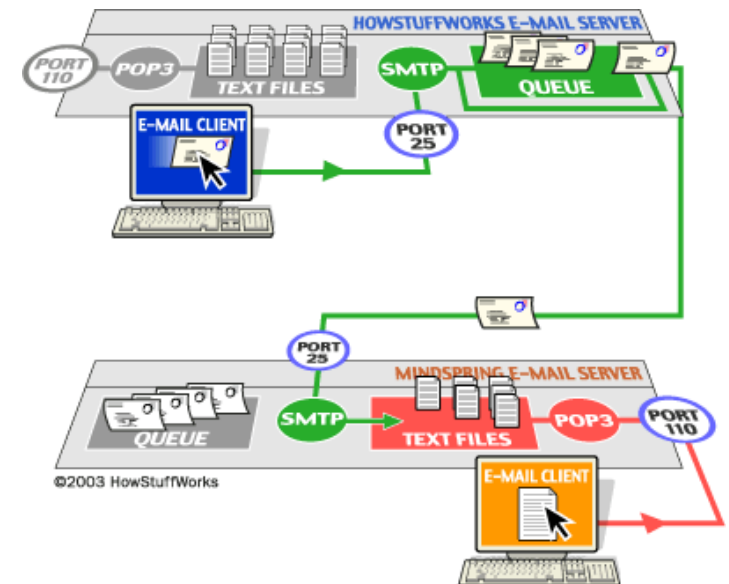
- Internet Abuse Investigations
- Firstly – what constitutes ‘abuse’- you must be versed with the laws of your state and the corporate policies
- As the forensics expert, you need the following:
 - your analysis toolkit (ProDiscover, X-Ways Forensics, EnCase, FTK etc.)
 - the organization’s Internet server logs (from the administrator):
 - the suspect computer’s IP address (from the administrator):
 - all the disk drives

 - mirror copy
 - history/ temp cache: compare with logs
 - time and frequency of visits
 - download information

 - AND???

Employee Termination Cases

- Email/ IM/ Text Abuse Investigations
 - most often include emails that are inappropriate, threats, harassments
 - e.g. Detroit mayor: <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503043.html>
- As the forensics expert, you need the following:
 - electronic copies of emails (header data)
 - phone records for texts – what are you looking for here?
 - email server logs – or the server that houses back ups
 - .pst files (Outlook)
 - company policies
 - What else?



Media Leak

- Why is the leaking of information a critical problem for many organizations?
 - 60% of employees who leave or are fired from their jobs, steal data:
 - <http://www.washingtonpost.com/wp-dyn/content/article/2009/02/26/AR2009022601821.htm>

- As the forensics expert, you need to do the following:
 - examine both internal and external communications of suspect's computer
 - search keywords – for related company products/ competitors. manufacturer/ media outlets
 - look through server logs – URL searches
 - email contact lists
 - phone records

 - corroborate dates of emails sent and significant events

 - recent example: http://www.mercurynews.com/breaking-news/ci_13663296?nclick_check=1



Industrial Espionage

- Involves either previously “trusted” employees or disgruntled employees or seemingly ignorant employees.
 - Coca-Cola example: <http://www.cybercrime.gov/dimsonind.htm>
- These are most often treated as criminal investigations
- As the forensics expert, you need to do the following:
 - examine all email/ download records of suspects
 - server logs
 - print jobs
 - related Internet newsgroups/ message boards for postings/ inquiries
 - surveillance cameras
 - phone records



© Coca-Cola Ltd.

