



# Performing a Security Forensics Review

VASCAN Educational Seminar

**Jeff Recor**

Olympus Security Group, Inc.  
[Jrecor@olympusecurity.com](mailto:Jrecor@olympusecurity.com)  
[www.olympusecurity.com](http://www.olympusecurity.com)

**Brian Gawne**

Olympus Security Group, Inc.  
[Bgawne@olympusecurity.com](mailto:Bgawne@olympusecurity.com)  
[www.olympusecurity.com](http://www.olympusecurity.com)



# Speakers

- **Jeff Recor:** CISSP, CISA, CISM, CFE, CPP, NSA IAM
  - 20 Years of experience
  - Walsh College IAC Director
  - President, Olympus Security Group, Inc.
  
- **Brian Gawne:** CISSP, CISA, CISM, EnCE
  - 15 Years of experience
  - Walsh College IAC Assistant Director
  - Vice President, Olympus Security Group, Inc.



# Goals Today

1. Present fundamentals of digital forensics
2. Showcase common tools and techniques
3. Discuss selected business case scenarios



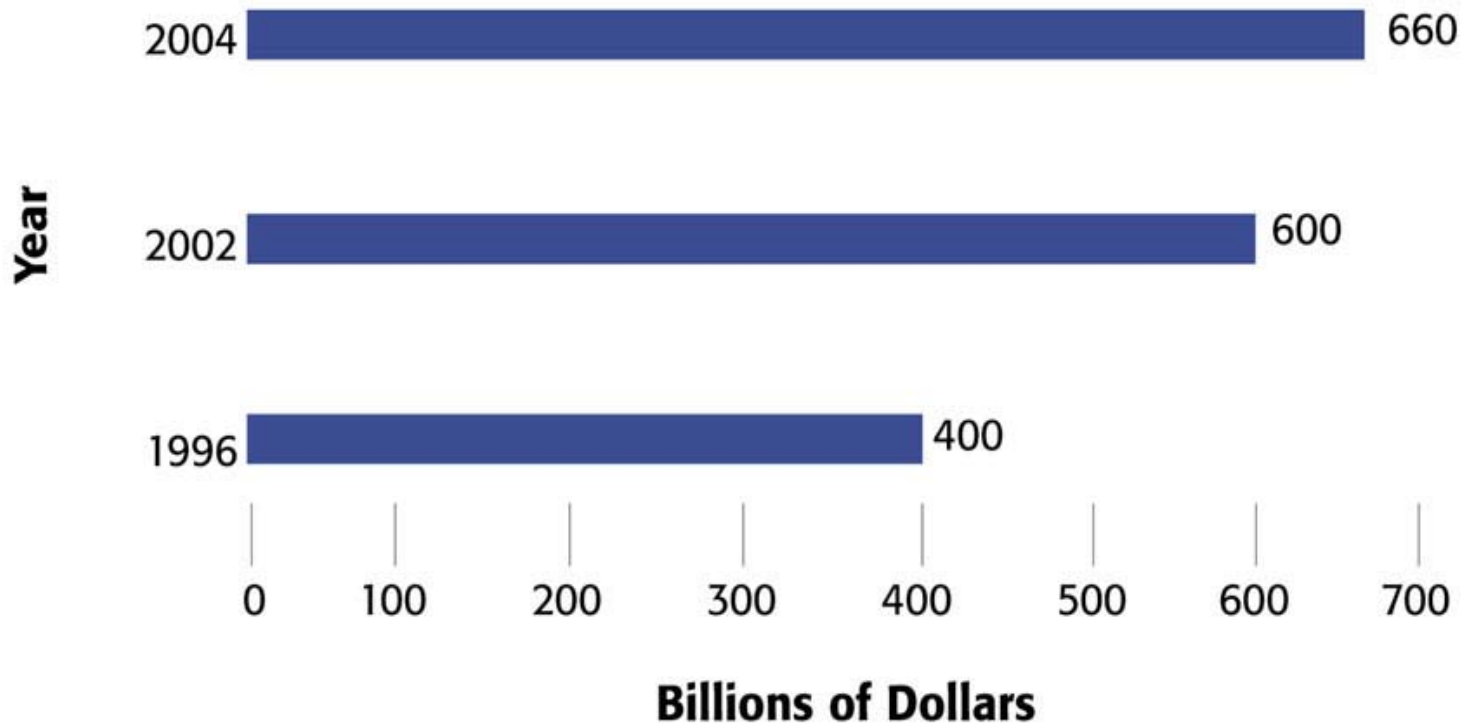
# Agenda

- How Bad is it
- Forensics basics
- Developing an investigation
- Working with law enforcement
- Pursuing civil and criminal actions against offenders



# ACFE Fraud Report 2005

## Total Occupational Fraud Losses <sup>3</sup>





## Frequency and Median Loss of Occupational Frauds Based on Industry

INDUSTRY	# CASES	% CASES <sup>2</sup>	MEDIAN LOSS
Manufacturing	65	12.9%	\$125,000
Banking	56	11.1%	\$101,000
Service	56	11.1%	\$139,000
Government	53	10.5%	\$45,000
Other	47	9.3%	\$145,000
Insurance	46	9.1%	\$172,500
Retail	40	7.9%	\$35,500
Health Care	37	7.3%	\$105,000
Education	31	6.1%	\$31,000
Construction	17	3.4%	\$145,000
Transportation	17	3.4%	\$225,000
Oil & Gas	16	3.2%	\$101,500
Communication	13	2.6%	\$150,000
Utility	13	2.6%	\$30,000
Real Estate	11	2.2%	\$385,000
Agriculture	6	1.2%	\$1,080,000



# FUD

- Hacker steals passwords from MIT, Cal Berkeley, U of MI, U of Toronto and Stanford...
- Ivy League hacking each other...
- Florida International ID Theft
- <http://security.duke.edu/0305.html>



# Common Myths

- “It is an art...”
- “... consult with trained professionals”
- “you don’t want your administrators to do forensics”
- [United States Secret Service](#)



# Soft Skills

- **Comfort with learning new things**
- **Inquisitive**
- **Communication**
- **Work Ethic**
- **Creature of habit**



# Hard Skills

- Technically competent
- Curious about technology
- Unix & Variants navigation
- Windows is a given...
- Ability to play poker
- Interview skills



# Certifications

- **Certified Computer Examiner (CCE)**
- **EnCase (EnCE)**
- **Misc Vendors**
- **Law Enforcement**
- **(off-shoots) CFE, CISA, etc**



# Forensics

- Is the collection, preservation, identification, extraction, analysis, documentation, and court presentation of electronic evidence.



# Types of Scenarios

- **Internal Employee(s)**
- **External**
  - Competitive Intelligence
  - Outright IP theft
- **Organized Crime**
- **State Sponsored**
- **Data Mercenary**



# High-Level Challenges

- **Competent criminals**
- **unaware lawyers/judges/law enforcement/practitioners**
- **Cost Driven Decision**
- **Technology**
- **Apathy**



- Use of Steganography:
  - **Steganography is the art and science of communicating in a way which hides the existence of the communication... The goal of steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present."**

[Markus Kuhn 1995-07-03].



# Unaltered photo...



This is a picture of  
My 4 year old. This  
Picture is  
completely  
unaltered...



# Altered Photo...



The text reads...

“This is text to show what Steganography can do- and how it works for my Walsh BIT 646 class.”

Jeff Recor



Unaltered photo



Altered photo





# Steganography

- **Steganography + Encryption =  
Big trouble for law enforcement!**



# Steganography Tools

- **Software (Commercial)**
  - Stealthencrypt
  - DataMark Technologies
- **Software (Freeware)**
  - Hide and Seek
  - White Noise Storm
  - S-Tools
  - StegoDos



# Forensics 101



# Mind Set

**Treat every incident  
as if it will end up  
in a court of law.**



# Basic Concerns

- Triage versus evidence collection
- If the computer is on, do I turn it off?
- How do I examine data for malicious activity?
- Hackers are bad guys!!



# Example Case #1

- A system administrator from another college calls and says someone from your network is hacking them...
- What do you do?



# Key Terms

- **Digital Evidence:** any data using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense



# Key Terms

- **3 Groups of systems:**
  - Open Computer Systems
  - Communication Systems
  - Embedded Computer Systems



# Evidence?

- Computer intrusions
- Fraud
- Intellectual property theft
- Child porn
- Stalking / harassment
- Violent crimes



# Policy/Law

- Federal / States / Local laws
- No uniform approach or “precedent”
- Privacy ?
- Judges / prosecutors / defense
- Jurisdiction



# Process

- There is a standardized “approach” to performing digital forensic investigations...



# Determine equipment affected

- The question is which system(s) need to be investigated?
  - Systems that are the known source of the incident
  - Systems that are the victims (these systems may point you to the source of the incident)



# Securing the Scene

- Determine what equipment is affected
- Document the Scene
- Video and/or photographs of the scene
- Make sure you limit entrance and exit to one door only (if possible), this will help control the removal of potential evidence



# Document the Scene

- It is very important to show the environment that these systems were in.
- Use Video or Photographs to document the environment.
- Start with the big picture and move in to each system. Take pictures of physical connections



# Document the Scene Cont.

- Documentation is key, so document everything even as you take pictures or video.
- Document condition of systems, how cables were connected, type of rack the system was located in, location of the rack in the room, etc...



# Gathering Of Evidence

- Determine how to collect necessary evidence
- Labeling of Evidence
- Documentation of Evidence Handling

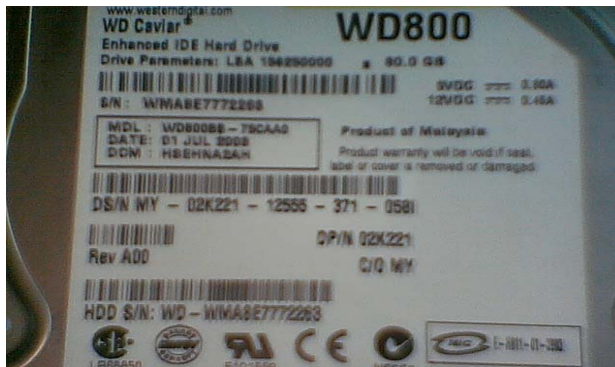
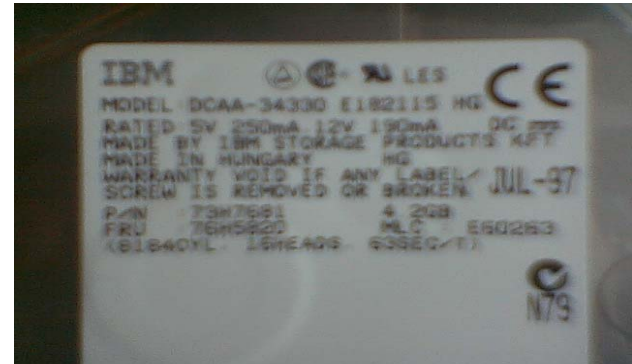




# Documentation of Evidence

- *Chain of Custody*
  - Is a simple yet effective process of documenting the complete journey of your evidence during the life of a case.
  - Detailed documentation of collection, safeguarding, and analysis of evidence.

# Documentation Example





# Labeling of Evidence

- Every piece of evidence which is removed from a site must be identified and labeled
- Using a label maker with self adhesive security labels make the task easier
- Record information about the device for documentation purposes, i.e. serial number, model, and manufacture



# Documentation of Evidence Handling

- Create an Excel spreadsheet or create a table to document evidence handling.
- Table should include:
  - Who Collected it
  - How and Where
  - Who took Possession of it
  - Serial Number
  - Description of evidence



# Storage of Evidence

- Evidence handling
- Controlled Storage
- Physical Access
- Documentation of Storage



# Evidence Handling

- Take precaution when moving evidence, typically evidence is not made to be moved.
  - Use padded containers for shipping
  - Use of static free packaging
- Remember to seal all containers and packaging and place a signature across the seal to ensure no one has tampered with the evidence



# Controlled Storage

- Keys for good evidence storage:
  - Cool and dry environment
  - Location should be large enough to accommodate all evidence in the packaging it was placed in



# Physical Access

- Should be a restricted area
- Area must be locked at all times
- If possible area should have proper protection against potential fire, flood, or other natural disaster



# Documentation of Storage

- A log should be kept of all access to the into the evidence storage location
- This log should include the following
  - Date
  - Time
  - Reason for entry
  - Name
  - Serial number of equipment removed
  - Description of equipment removed



# Documentation of Evidence Handling

- Once the evidence has been collected documentation must be kept in order to track when it was moved from storage
- This is crucial to prove Chain of Custody



# Documentation of Evidence Handling Cont.

- Below is an example of an Evidence Handling document

Item	Date	Time	Location	Name	Reason
Toshiba Tecra 8000 serial #1234	2/7/2002	9:30 AM	Locked cabinet in room A	Smith	Safe Keeping
Toshiba Tecra 8000 serial #1234	2/8/2002	1:00 PM	Removed from locked cabinet	Smith	Analysis
Toshiba Tecra 8000 serial #1234	2/8/2002	9:00 PM	Returned to locked cabinet in room A	Smith	Safe Keeping



# Evidence Acquisition

- Utilizing a forensically sound method of obtaining a bit level image of the evidence.
- Multiple tools available.



# Detailed Challenges

- Messy form of evidence
- Digital evidence is generally an abstract of an event or object
- Digital evidence can be easily manipulated
- Evidence is usually circumstantial



## Example Case #2

- A co-worker from another department tells you they suspect one of their employees is looking at pornography?
- What do you do?



# System Devices

- PDA
- Laptop
- Desktop
- Servers
- Infrastructure (router, switches, etc)
- Cameras
- MP3 Players
- Phone Systems
- Voice Mail Systems



# Evidence Orientation

- Determine Operating System
- Verify Email applications
- Search for web mail usage
- Hidden files
- Location of user files



# Image of effected system

- In order to preserve evidence you never want to perform analysis on the original hard drive of the system we need to do the following
  - Image of original hard drive
  - Image of the 1<sup>st</sup> backup hard drive
- This allows the investigator to perform the analysis with the ability to restore the data over and over again without affecting the original



# Electronic Finger Printing

- Is one way to prove that the evidence was not altered or changed in anyway after it was collected
- In order to provide this proof we would use a cryptographic technique, and the value is called a hash



# Electronic Finger Printing Cont.

- **Cryptography** – The art of protecting information by transforming it (*encrypting* it) into an unreadable format, called cipher text
- **Hash** - Hashes play a role in security systems where they're used to ensure that data has not been tampered with. The sender generates a hash of the data, and encrypts it.



# Examination of the partition table

- Examination of the partition table is done to do the following
  - Determine what type of partition tables are configured on the system (i.e. NTFS, FAT, FAT32, etc)
  - Determine what types of tools you will be able to use on the hard drive for the analysis



# Digital Signature of Hard Drive

- Same process as Electronic Finger Printing, only it is done is to the entire hard drive
- This is used to prove the hard drive under analysis is an exact copy of the original hard drive
- These steps as well as everything else should be documented



# Directory listings

- This is typically done to determine what you are up against
- Dump a directory listing to a file, printer, or export to excel





# Search Definition

- Can include
  - Keyword searches
  - File Signature Analysis
  - Recovery of deleted files



# Initial Findings

- These findings may point you in another direction to take the investigation
- Or End the investigation all together



# Search Definition Refinement

- New search term can be determined during review of previous search results
- New search methods can be used



# Findings Review

- During each phase of the investigation findings are reviewed with client and attorney's.



# Analysis

- Image of effected system
- Digital Signature of hard drive
- Examination of the partition table
- Directory listings



# Tools Example





# Developing an Investigation



# Mind Set

**Treat every incident  
as if it will end up  
in a court of law.**



# Developing an Investigation

- Why Investigate
- Justification for Investigation
- Who to involve in the investigation



# Developing an Investigation Cont.

- Questions to Answer
  - Authority
  - Obligations/Goals
  - Reporting
  - Escalation
  - Investigation Length
  - Steps to consider



# Why Investigate?

- **Some typical reasons for Investigation:**
  - Internet usage exceeds norm
  - Using email inappropriately
  - Theft of information
  - Violation of security policies or procedures
  - Intellectual property infractions



# Justification for Investigation

- Often include a misuse or violation of:
  - Company policies and procedures
  - Legal Statutes
  - Regulatory Statutes
  - Mandatory Statutes



# Who to involve in the Investigation

- Depending on the type and origin of the complaint the following departments may need to be included:
  - Internal Audit
  - Network/Operations
  - Data Security
  - Physical Security
  - Human Resources
  - Legal
  - External Consultants
  - External law enforcement



# Questions to Answer - Authority

- Determine your level of authority for the investigation. Will you be granted access to:
  - Information
  - Resources (not just personnel)
  - Restricted area of the company
  - Requests interview with personnel



# Questions to Answer - Obligations/Goals

- Determine how to handle the situation in case the investigation leads to your supervisor.
- How to handle the potential uncovering of illegal activity



# Questions to Answer - Reporting

- Determine whom you are to report your findings to.
- Determine how these findings are to be reported.



# Questions to Answer - Escalation

- Before beginning an investigation determine the escalation path in case of any of the following circumstances
  - Cooperation
  - Legal issues
  - Confidential Information
  - Human Resource Issues



# Questions to Answer - Length of Investigation

- In order to plan the investigation properly set milestones.
- Note the progress of these milestones in status reports to management



# Questions to Answer - Steps to consider

- Review the filed complaint
- Determine authenticity of complaint
- Review policies, procedures, and legal statutes
- Plan investigation
- Determine the feasibility/impact of conducting investigation or not
- Obtain management's approval to proceed with the investigation
- Contact departments involved



# Working with Law Enforcement



# Working with Law Enforcement

- Things to do before hand
- Things to consider
- Which "Geeks with guns" to involve



# Things to do before hand

- Confer with corporate legal consul
- Receive management approval
- Prepare public relations for possibility of negative impact if/when this becomes public



# Things to consider

- **Loss of control of the investigation**
  - Remind law enforcement that you are the victim.
  - Don't be afraid to ask about the status of the investigation.



# Things to consider Cont..

- **Cost and Time**
  - Be prepared to assist fully in the investigation and following prosecution.
  - Keep track of cost associated with the investigation (ie – replacement hardware, consulting time, cost of other materials, etc)



# When to involve “Geeks with guns”?

- Be prepared to answer questions:
  - Has there been a delay in reporting this crime?
    - If so Why?
  - Who knows about the crime?
    - Why?
  - Has there been an internal investigation?
    - If so, who conducted it and what were the results?
  - Have you identified a potential suspect?
    - Has anyone suspected been confronted?





# Forensics Books

- **Computer Forensics – Incident Response Essentials**
  - Warren G. Kruse, Jay g. Heiser
  - ISBN: 0-201-70719-5
- **Cyber Forensics – A field manual for Collecting, Examining, and Preserving Evidence of Computer Crimes**
  - Albert J. Marcella, Robert S. Greenfield
  - ISBN: 0-84943-0955-7



# Question and Answer

