Digital investigations have matured

The field of computer forensics is still a relatively new discipline, and is constantly evolving. A combination of law and computer science, the field is defined as the practice of gathering and examining data from computer systems, networks and wireless devices in a way that, if necessary, will hold up as evidence in a court.

Historically driven by human relations and legal issues, digital investigations are now increasingly being launched following data breaches and suspected computer intrusions, experts say.

*With the frequency and sophistication of today’s cyberattacks, computer forensics has become an integral aspect of information security incident response plans, especially for those in government and the technology and defense industries.*

“Digital forensics in IT security is necessary to provide a new component called threat intelligence,” says Rob Lee, faculty lead for digital forensics at the SANS Institute.

Lack of investigation means that potential vectors of attack are not shored up and future penetration is possible or the threat persists,” the report states. “Insiders are not identified, and incongruities are not investigated to identify a larger threat.”

http://www.scmagazine.com.au
Bin Laden's Computers Will Test U.S. Forensics

For the U.S. government, the raid on Osama bin Laden's compound in Pakistan represents a unique opportunity to test advanced computer forensics techniques called "media exploitation" that it's developed over the last few years. While the U.S. government isn't exactly volunteering what's happening now, the Army has confirmed in the past that it provides "tactical DOMEX teams" to troops in Afghanistan. And a Defense Department directive (PDF) from January 2011 says the National Media Exploitation Center, or NMEC, will be the "central DoD clearinghouse for processing DoD-collected documents and media," a category that would include the bin Laden files.

An initial forensic analysis of bin Laden's hard drives will likely be done with keyword searches in Arabic and English. "You can get thousands of hits," Mark McLaughlin, president of Santa Monica, Calif.-based Computer Forensics International, told CNET. "Those hits need to be looked at individually, and in context," he said, which can take a while.

U.S. officials are calling the data a potential treasure trove of information on al Qaeda's current and planned operations, perhaps the most important since 9/11. They're hoping it could yield hints about the whereabouts of Ayman al-Zawahiri, bin Laden's chief lieutenant.
Module Objectives

- Computer Forensics
- Evolution of Computer Forensics
- Objective of Computer Forensics
- Benefits of Forensics Readiness
- Forensics Readiness Planning
- Cyber Crimes
- Types of Computer Crimes
- Cyber Crime Investigation

- Key Steps in Forensics Investigation
- Role of Forensics Investigator
- Accessing Computer Forensics Resources
- Role of Digital Evidence
- Understanding Corporate Investigations
- Enterprise Theory of Investigation (ETI)
- Legal Issues
- Reporting the Results
Forensics Science

Definition
Application of physical sciences to law in the search for truth in civil, criminal, and social behavioral matters to the end that injustice shall not be done to any member of society.

Aim
Determining the evidential value of the crime scene and related evidence.
Computer Forensics

A methodical series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media, that can be presented in a court of law in a coherent and meaningful format.

- Dr. H.B. Wolfe

The preservation, identification, extraction, interpretation, and documentation of computer evidence, to include the rules of evidence, legal processes, integrity of evidence, factual reporting of the information found, and providing of expert opinion in a court of law or other legal and/or administrative proceeding as to what was found.

- CSI

Forensics Computing is the science of capturing, processing, and investigating data from computers using a methodology whereby any evidence discovered is acceptable in a Court of Law.
Security Incident Report

- Companies that had a security incident in the last year:
  - Small Organizations (<50 staff): 83%
  - Large Organizations (>250 staff): 92%

- Average (median) number of breaches in the last year:
  - Small Organizations (<50 staff): 14
  - Large Organizations (>250 staff): 45

- Average cost of a worst incident of the year:
  - Small Organizations (<50 staff): $45.2k - $90.5k
  - Large Organizations (>250 staff): $726,492.43 - $1,792,553.50

Information Security Breaches Survey 2010, by PricewaterhouseCoopers (PwC)
Aspects of Organizational Security

1. IT Security
   - Application security
   - Computing security
   - Data security
   - Information security
   - Network security

2. Physical Security
   - Facilities security
   - Human security
   - Border security
   - Biometric security

3. Financial Security
   - Security from frauds
   - Phishing attacks
   - Botnets
   - Threats from cyber criminals
   - Credit card fraud

4. Legal Security
   - National security
   - Public security
   - Defamation
   - Copyright information
   - Sexual harassment
Evolution of Computer Forensics (Cont’d)

- Francis Galton (1822-1911)
  - Made the first recorded study of fingerprints

- Leone Lattes (1887-1954)
  - Discovered blood groupings (A, B, AB, and O)

- Calvin Goddard (1891-1955)
  - Allowed firearms and bullet comparison for solving many pending court cases

- Albert Osborn (1858-1946)
  - Developed essential features of document examination

- Hans Gross (1847-1915)
  - Made use of scientific study to head criminal investigations

- FBI (1932)
  - A lab was set up to provide forensic services to all field agents and other law authorities across the country
Evolution of Computer Forensics

1984
Computer Analysis and Response Team (CART) was developed to provide support to FBI field offices in the search of computer evidence

1993
First International Conference on computer evidence was held

1995
International Organization on Computer Evidence (IOCE) formed

1998
International Forensic Science Symposium (IFSS) formed to provide forum for forensic manager

2000
First FBI Regional Computer Forensic Laboratory was established
Objective of Computer Forensics

To recover, analyze, and preserve computer and related materials in such a way that they can be presented as evidence in a court of law.

To identify the evidence quickly, estimate the potential impact of the malicious activity on the victim, and assess the intent and identity of the perpetrator.
Need for Computer Forensics

1. To ensure the overall **integrity** and the continued existence of an organization’s computer system and network infrastructure.

2. To extract, process, and interpret the factual evidence so that it proves the **attacker’s actions in the court**.

3. To efficiently **track down perpetrators** from different parts of the world.

4. To protect the organization’s **money** and valuable time.
Module Flow

- Computer Forensics
- Forensics Readiness
- Cyber Crimes
- Cyber Crime Investigation
- Corporate Investigations
- Reporting a Cyber Crime
Benefits of Forensics Readiness

1. Evidence can be gathered to act in the company's defense if subject to a lawsuit.

2. In the event of a major incident, a fast and efficient investigation can be conducted and corresponding actions can be followed with minimal disruption to the business.

3. Forensic readiness can extend the target of information security to the wider threat from cybercrime, such as intellectual property protection, fraud, or extortion.

4. Fixed and structured approach for storage of evidence can considerably reduce the expense and time of an internal investigation.

5. It can improve and simplify law enforcement interface.

6. In case of a major incident, proper and in-depth investigation can be conducted.
Goals of Forensics Readiness

To collect acceptable evidence without interfering with the business processes

To gather evidence targeting the potential crimes and disputes that may adversely impact an organization

To ensure that evidence makes a positive impact on the outcome of any legal action

To allow an investigation to proceed at a cost in proportion to the incident
Forensics Readiness Planning

- Define the business states that need digital evidence
- Identify the potential evidence available
- Determine the evidence collection requirement
- Decide the procedure for securely collecting the evidence that meets the requirement in a forensically sound manner
- Establish a policy for securely handling and storing the collected evidence
- Ensure that the observation process is aimed to detect and prevent the important incidents
- Ensure investigative staff are capable to complete any task related to handling and preserving the evidence
- Document all the activities performed and their impact
- Ensure authorized review to facilitate action in response to the incident
Cyber Crime

Cyber crime is a term used broadly to describe criminal activity in which computers or networks are a tool, a target, or a place of criminal activity. These categories are not exclusive and many activities can be characterized as falling in one or more categories.

Cyber crime is defined as any illegal act involving a computer, its systems, or its applications.

- Crime directed against a computer
- Crime where the computer contains evidence
- Crime where the computer is used as a tool to commit the crime

A Cyber crime is intentional and not accidental.
Computer Facilitated Crimes

- Dependency on the computer has given way to new crimes
- Computer crimes pose new challenges for investigators due to their:
  - Speed
  - Anonymity
  - Fleeting nature of evidence
Modes of **Attacks**

Cyber crime can be categorized into two types based on the **line of attack**

- **Insider Attacks**
  - Breach of trust from employees within the organization

- **External Attacks**
  - Attackers either hired by an insider or by an external entity to **destroy the competitor’s reputation**
Examples of Cyber Crime (Cont’d)

- Fraud achieved by the manipulation of the computer records
- Spamming wherever outlawed completely or where regulations controlling it are violated
- Deliberate circumvention of the computer security systems
- Unauthorized access to or modification of programs and data
- Intellectual property theft, including software piracy
- Industrial espionage by means of access to or theft of computer materials
Examples of Cyber Crime

- Identity theft, which is accomplished by the use of fraudulent computer transactions
- Writing or spreading computer viruses or worms
- Salami slicing is the practice of stealing money repeatedly in small quantities
- Denial-of-service attack, where the company’s websites are flooded with service requests and their website is overloaded and either slowed or is crashed completely
- Making and digitally distributing child pornography
# Types of Computer Crimes

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Theft</td>
<td>Credit Card Fraud</td>
<td>Internet Extortion</td>
</tr>
<tr>
<td>Hacking</td>
<td>On-Line Auction Fraud</td>
<td>Investment Fraud</td>
</tr>
<tr>
<td>Computer Viruses</td>
<td>Email Bombing and SPAM</td>
<td>Escrow Services Fraud</td>
</tr>
<tr>
<td>Cyber Stalking</td>
<td>Theft of Intellectual Property</td>
<td>Cyber Defamation</td>
</tr>
<tr>
<td>Drug Trafficking</td>
<td>Denial of Service Attack</td>
<td>Software Piracy</td>
</tr>
<tr>
<td>Phishing/Spoofing</td>
<td>Debt Elimination</td>
<td>Counterfeit Cashier's Check</td>
</tr>
<tr>
<td>Wrongful Programming</td>
<td>Web Jacking</td>
<td>Embezzlement</td>
</tr>
</tbody>
</table>

1. **Computer Crime**
Cyber Criminals

Cyber criminals are increasingly being associated with organized crime syndicates to take advantage of their sophisticated techniques.

There are organized groups of cyber criminals who work in a hierarchical setup with a predefined revenue sharing model, like a major corporation that offers criminal services.

Organized groups create and rent botnets and offer various services, from writing malware, to hacking bank accounts, to creating massive denial-of-service attacks against any target for a price.

According to Verizon's 2010 Data Breach Investigations Report, the majority of breaches were driven by organized groups and almost all data stolen (70%) was the work of criminals outside the victim organization.

The growing involvement of organized criminal syndicates in politically motivated cyber warfare and hactivism is a matter of concern for national security agencies.
Organized Cyber Crime: Organizational Chart

Criminal Boss

Underboss: Trojan Provider and Manager of Trojan Command and Control

Attackers Crimeware Toolkit Owners

Trojan Distribution in Legitimate Website

Campaign Manager

Campaign Manager

Campaign Manager

Affiliation Network

Affiliation Network

Affiliation Network

Stolen Data Reseller

Stolen Data Reseller

Stolen Data Reseller
How Serious are Different Types of Incidents?

Information Security Breaches Survey 2010, by PricewaterhouseCoopers (PwC)
Disruptive Incidents to the Business

- Virus infection or disruptive software: 11% Very Major, 18% Major, 38% Minor
- Systems failure or data corruption: 12% Very Major, 37% Major, 41% Minor
- Staff misuse of information systems: 14% Very Major, 20% Minor
- Unauthorized access by outsiders (including hacking attempts): 4% Very Major, 32% Major, 20% Minor
- Physical theft of computer equipment: 3% Very Major, 28% Minor
- Computer fraud or confidentiality breach: 4% Very Major, 27% Minor

Information Security Breaches Survey 2010, by PricewaterhouseCoopers (PwC)
Cost Expenditure Responding to the Security Incident

ISBS 2010 - large organizations
- 26% (£1 - £999)
- 24% (£1,000 - £9,999)
- 10% (£10,000 - £49,999)
- 4% (£50,000 - £99,999)
- 3% (£100,000 - £249,999)
- 1% (£250,000 - £499,999)
- 2% More than £500,000

ISBS 2010 - small organizations
- 35% (£1 - £999)
- 11% (£1,000 - £9,999)
- 4% (£10,000 - £49,999)
- 1% (£50,000 - £99,999)
- 1% (£100,000 - £249,999)
- 2% £250,000 - £499,999

ISBS 2008 - overall
- 25% (£1 - £999)
- 12% (£1,000 - £9,999)
- 2% (£10,000 - £49,999)

ISBS 2006 - overall
- 31% (£1 - £999)
- 8% (£1,000 - £9,999)

Information Security Breaches Survey 2010, by PricewaterhouseCoopers (PwC)
Module Flow

- Computer Forensics
- Forensics Readiness
- Cyber Crimes
- Cyber Crime Investigation
- Corporate Investigations
- Reporting a Cyber Crime
Cyber Crime Investigation

The investigation of any crime involves the painstaking collection of clues and forensic evidence, particularly for white collar crime, where documentary evidence plays a crucial role.

It is inevitable that there will be at least one electronic device found during the course of an investigation.

The information held on the computer may be crucial and must be investigated in the proper manner, especially if any evidence found is to be relied upon in the court of law.

It may be a computer, printer, mobile phone, or a personal organizer.
Key Steps in Forensics Investigation (Cont’d)

1. Identify the computer crime
2. Collect preliminary evidence
3. Obtain court warrant for seizure (if required)
4. Perform first responder procedures
5. Seize evidence at the crime scene
6. Transport evidence to the forensic laboratory
7. Create two bit stream copies of the evidence
8. Generate MD5 checksum on the images
Key Steps in Forensics Investigation

9. Maintain a chain of custody

10. Store the original evidence in a secure location

11. Analyze the image copy for evidence

12. Prepare a forensic report

13. Submit the report to the client

14. If required, attend the court and testify as an expert witness
Rules of Forensics Investigation

- Minimize the option of examining the original evidence
- Follow rules of evidence
- Do not tamper with the evidence
- Always prepare for a chain of custody
- Handle evidence with care
- Never exceed the knowledge base
- Document any change in evidence
Need for Forensics Investigator

Examination of a computer by a technically inexperienced person will almost always result in rendering any evidence found inadmissible in a court of law.
Role of Forensics Investigator

1. Protects the victim’s computer from any damage and viruses
2. Determines the extent of damage
3. Gathers evidence in a forensically sound manner
4. Analyzes the evidence data found and protects it from damage
5. Prepares the analysis report
6. Presents acceptable evidence in the court
Accessing Computer Forensics Resources

You can obtain resources by joining various discussion groups such as:

- Computer Technology Investigators Northwest
- High Technology Crime Investigation Association

Joining a network of computer forensic experts and other professionals

News devoted to computer forensics can also be a powerful resource

Other resources:

- Journals of forensic investigators
- Actual case studies
Role of Digital Evidence

Examples of cases where digital evidence may assist the forensic investigator in prosecution or defense of a suspect:

- Names and addresses of contacts
- Malicious attacks on the computer systems themselves
- Records of movements
- Unauthorized transmission of information
- Theft of commercial secrets
- Use/abuse of the Internet
- Production of false documents and accounts
- Encrypted/password protected material
- Abuse of systems
- Email contact between suspects/conspirators
Understanding Corporate Investigations

- Involve private companies who address company’s policy violations and litigation disputes.
- Company procedures should continue without any interruption from the investigation.
- After the investigation, the company should minimize or eliminate similar litigations.
- Industrial espionage is the foremost crime in corporate investigations.
1. An incident occurs in which the company’s server is compromised

2. The client contacts the company’s advocate for legal advice

3. The advocate contacts an external forensic investigator

4. The forensic investigator prepares first response of procedures (FRP)

5. The forensic investigator (FI) seizes the evidence at the crime scene and transports it back to the forensics lab

6. The forensic investigator prepares the bit-stream images of the file

7. The forensic investigator creates an MD5 of the files
Approach to Forensics Investigation: A Case Study

- The forensic investigator examines the evidence files for proof of a crime.
- The FI prepares investigation reports, concludes the investigation and enables the advocate to identify the required proofs.
- The FI handles the sensitive report of the client in a secure manner.
- The advocate studies the report and might press charges against the offensive in the court of law.
- The forensic investigator usually destroys all the evidence.

CHFI
43
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Instructions for the **Forensic Investigator** to Approach the Crime Scene

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any liabilities from the incident and how they can be managed</td>
</tr>
<tr>
<td>2</td>
<td>Finding and prosecuting/punishing (internal versus external culprits)</td>
</tr>
<tr>
<td>3</td>
<td>Legal and regulatory constraints on what action can be taken</td>
</tr>
<tr>
<td>4</td>
<td>Reputation protection and PR issues</td>
</tr>
<tr>
<td>5</td>
<td>When to advise partners, customers, and investors</td>
</tr>
<tr>
<td>6</td>
<td>How to deal with employees</td>
</tr>
<tr>
<td>7</td>
<td>Resolving commercial disputes</td>
</tr>
<tr>
<td>8</td>
<td>Any additional measures required</td>
</tr>
</tbody>
</table>
Why and When Do You Use Computer Forensics?

**Why?**
- Gather evidence of computer crimes in a forensically sound manner
- To protect organization from similar incidents in future
- To minimize the tangible and intangible losses to the organization
- To support prosecution of perpetrator of an incident

**When?**
- If a breach of contract occurs
- If copyright and intellectual property theft/misuse happens
- Employees’ disputes
- Damage to resources
Enterprise Theory of Investigation (ETI)

By applying the ETI with favorable state and federal legislation, law enforcement can target and dismantle entire criminal enterprises in one criminal indictment.

Rather than viewing criminal acts as isolated crimes, the ETI attempts to show that individuals commit crimes in furtherance of the criminal enterprise itself; which means individuals commit criminal acts solely to benefit their criminal enterprise.
Legal Issues

- It is not always possible for a computer forensics expert to separate the legal issues surrounding the evidence from the practical aspects of the computer forensics.
  - Ex: The issues related to authenticity, reliability and completeness, and convincing.
- The approach of investigation diverges with changes in technology.
- Evidence shown is to be untampered with and fully accounted for, from the time of collection to the time of presentation to the court; hence, it must meet the relevant evidence laws.
Reporting the **Results**

- Report should consist of **summary of conclusions, observations**, and all appropriate recommendations.

- Report is based on:
  - Who has access to the data?
  - How could it be made available to an investigation?
  - To what business processes does it relate?

A good investigation report contains:

- Methods of investigation
- Adequate supporting data and data collection techniques
- Calculations used and error analysis
- Results and comments
- Graphs and statistics
- References and appendices
- Acknowledgements
- Litigation support reports
Module Flow

- Computer Forensics
- Forensics Readiness
- Cyber Crimes
- Cyber Crime Investigation
- Corporate Investigations
- Reporting a Cyber Crime
Why you Should Report Cybercrime?

Companies might be reluctant to share information regarding the impact to their **business** and the **sensitivity of the data** involved.

Only by sharing information with law enforcement and appropriate industry groups, cyber criminals will be **identified and prosecuted**.

New cyber security threats will be identified, and successful attacks on **critical infrastructures and economy** will be prevented.

Law enforcement’s ability to **identify coordinated threats** is directly tied to the volume of reporting.
Internet-related crime, like any other crime, should be reported to appropriate law enforcement investigative authorities at the local, state, federal, or international levels, depending on the scope of the crime.

The primary federal law enforcement agencies that investigate domestic crime on the Internet include:

- Bureau of Alcohol, Tobacco and Firearms (ATF)
- Federal Bureau of Investigation (FBI)
- United States Postal Inspection Service
- United States Immigration and Customs Enforcement (ICE)
- United States Secret Service
Government Initiatives to Combat Cyber Crime

The Internet Crime Complaint Center (IC3) (Online reporting for Internet related crime)

Department of Homeland Security's National Infrastructure Coordinating Center: (202) 282-9201 (Report incidents relating to national security and infrastructure issues)

U.S. Computer Emergency Readiness Team (U.S. CERT) (Online reporting for technicians)

National Association of Attorney General (NAAG) (Computer Crime Point of Contact List)
Person Assigned to Report the Crime

- Have a single contact to whom employees should report **suspicious events** and who will track changes in contacts or procedures.
- Have a single contact who will report incidents to outside agencies, including law enforcement, regulatory bodies and information sharing organizations such as InfraGard and the **industry Information Sharing and Analysis Centers Council** (ISAC Council).
- Keep a list of the **incident response team** members’ names, titles and 24/7 contact information, along with their role in a security breach.
- Have contact information for vendors contracted to help during a **security emergency**, as well as ISPs and other relevant technology providers.

- Keep contact information for **major customers** and clients who might be affected.
- In advance, establish contacts at the relevant **law enforcement agencies**, typically:
  - The national infrastructure protection and computer intrusion squad at the local FBI field office.
  - The electronic crimes investigator at the local Secret Service field office.
  - The electronic crimes investigator at your local police.
- Keep their contact information easily accessible.
When and How to Report an Incident?

If an attack is under way, pick up the phone and call the previously established law enforcement contact immediately and communicate the basic information that is included in the CIO Cyber threat Response Form.

Additional information that will help law enforcement agents in their investigation:
- What are the primary systems involved?
- How was the attack carried out?
- What steps have you taken to mitigate or remediate?
- Does a suspect exist? If so, is it a current or former employee/contractor?
- What evidence is available to assist in the investigation (e.g., log files, physical evidence, etc.)?

To track the status of your case once you have filed a report, contact the field office that is conducting the investigation.
Who to Contact at the Law Enforcement?

1. There is no single answer for which law enforcement agency to contact in the event of a cyber-security breach.

2. The FBI and U.S. Secret Service share jurisdiction for computer crimes that cross state lines.

3. However, most law enforcement agencies, including the FBI and USSS, encourage people to:
   - Pre-establish contact with someone in law enforcement who is trained in and responsible for dealing with computer crime.
   - Work with the person or people you have the best relationship with.
Forensics computing is the science of capturing, processing, and investigating data from computers using a methodology whereby any evidence discovered is acceptable in a court of Law.

The need for computer forensics has increased due to the presence of a majority of the digital documents.

Cyber crime is defined as any illegal act involving a computer, its systems, or its applications.

Forensics results reports should consist of a summary of conclusions, observations, and all appropriate recommendations.
“Somebody broke into your computer, but it looks like the work of an inexperienced hacker.”
"No fingerprints, no picture ID, no Social Security number. I’m afraid your baby presents a serious security risk."