Research in Digital Forensics

Modern Digital Forensics
Modern Digital Forensics – What’s New

- New Intellectual property concerns
  - IP/Brand related abuse
  - File sharing and copyright violations

- Corporate reliance on Internet technology
  - Attacks over the Network
  - Technology-assisted Insider Threats
  - Internet fraud, phishing, infrastructure attacks
  - Computer related employee misconduct

- Corporate accounting scandals
  - Enron, Andersen, WorldCom, and others
  - Sarbanes–Oxley Act of 2002 (SOX) requiring digital evidence collection capability, investigation and incident response processes
Modern Digital Forensics

- A formal scientific discipline
  - Theory, Abstractions, Models, Frameworks
  - Corpus of literature and professional practice
  - Practical tools, methods, procedures
  - Confidence and trust in results

- Professional community
  - International peer reviewed journals and conferences
  - Practitioner best practice
  - Formal standards and procedures
Modern Digital Forensics

- Expanded scope of Digital Forensics: now includes
  - Software forensics (malware/code analysis)
  - Live system forensics (memory, running processes)
  - Network forensics (captured traffic, remote collection)
  - Host/Network Log & Data Correlation

- Smart & Embedded devices
  - Smart & mobile phones,
  - Pads, PDAs,
  - New capabilities Camera, GPS, WiFi, Motion sensors

- Arrival of anti-forensics or counter-forensics
Digital Forensics Today

- The current state of digital forensics
  - Thriving scientific research community
  - Experienced and professional community of practitioners
  - Rigorous and formalized processes and methodology
  - Well established fundamental tools and techniques
  - Significant growth in the corporate sector

- The coming decade: beyond 2010
  - What existing problems need solving?
  - What new expectations and requirements will be demanded?
  - Which challenges we must face and overcome?
  - How must digital forensics change and adapt?
Real World Challenges

- **Forensic Readiness**
  - Less reliance on accidentally found evidence, more preparedness and planning for evidence collection
  - Building forensic capability into IT infrastructure and applications as a standard component, from the initial design phase
  - Having processes, tools and trained staff available in advance, for performing forensic work

- **Information Security**
  - Forensic tools can be powerful and invasive
  - Must be carefully controlled and responsibly used
  - Policies to ensure access is restricted to authorized investigators and forensic analysts
  - Adequate protection of copied data during storage and transfer, in the short term as well as the long term
Real World Challenges

- **Legal and Regulatory Compliance**
  - Jurisdiction differences and forensic requirements are different around the world, complex to implement globally
  - Some forensic activity may be restricted: privacy law, wiretapping law, etc.
  - Some forensic activity may be mandated: data retention, evidence collection process, etc.

- **Risk sensitive forensics**
  - Balancing the cost and effort of forensic work with the likelihood of finding evidence
  - Technical depth: you can always dig deeper, but when do you stop?
Real World Challenges

- Adopting new cost effective and efficient solutions
  - Moving data to the tools vs. moving the tools to the data (for example: integrating e-discovery tools into backup systems)
  - Replacing suspect hard disks, instead of forensic imaging in the field
  - Separating forensic acquisition role from forensic analysis role

- New Technologies
  - VoIP vs Mobile vs Land-lines
  - Devices become more personal, privacy a concern
    - Increase in electronic data devices and storage which cannot be easily analyzed: iPhone, iPad, and other restricted access devices
  - Social networking sites, blogs, external public applications
Real World Challenges

- External ownership of corporate IT Infrastructure
  - Complex, multi-party infrastructure outsourcing
  - Externally hosted/shared applications
  - Cloud computing
  - Certain aspects of technical forensic computing may not be feasible or sensible in these environments

- Shift in evidence location
  - Less reliance on client PC disks as a regular evidence source, more reliance on server logs and archived data
  - Evidence increasingly found on external infrastructure, requiring cooperation with external parties
Real World Challenges

- **Ever Increasing data volume**
  - Large amounts of data can be collected from large corporate IT Infrastructures
  - Modern hard disk sizes: TBs are common, working with forensic images this size is cumbersome and time consuming
  - Large data sets require scalable and stable forensic tools
  - Improved reliance statistical analysis, anomaly detection, data mining, correlation
  - Data retention is a challenge: how long? how much detail?
Real World Challenges

- **Complexity of finding evidence**
  - Hard to maintain up-to-date forensic capability for rapidly changing technology
  - Many layers of data encapsulation and abstraction, increasing levels of technical detail
  - Difficulty analyzing proprietary, undocumented technologies
  - Encryption: secure email, protected files and file systems, key escrow/recovery processes

Anything more?
Overview of Forensics Process
Managing the Life-Cycle of a Case

A defensible (objective, unbiased) approach is:

- Performed in accordance with forensic science principles
- Based on standard or current best practices
- Conducted with verified tools to identify, collect, filter, tag and bag, store, and preserve e-evidence
- Conducted by individuals who are certified in the use of verified tools, if such certification exists
- Documented thoroughly
Preserving the chain of custody for e-evidence requires proving that:

- No information has been added, deleted, or altered in the copying process or during analysis
- A complete copy was made and verified
- A reliable copying process was used
- All media were secured
- All data that should have been copied have been copied
Managing the Life-Cycle of a Case (Cont.)

Many factors affect the choice of tools selected for a case:

- Type of device (What Types?)
- Operating system (Options?)
- Software applications (Why?)
- Hardware platforms (Why does it matter?)
- State of the data (What state can it be?)
- Domestic and international laws
- Concerns about bad publicity or liability
Many tools are freely available that help criminals hide evidence of cybercrimes

- Nuker
- Anonymous remailers
- Password cracker
- Scanner
- Spoofier
- Steganography
- Trojan horse
Investigation Objectives & Chain of Custody Practices

<table>
<thead>
<tr>
<th>Investigation Objectives</th>
<th>Chain of Custody Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document the scene, evidence, activities, and findings</td>
<td>Document everything that is done; keep detailed records and photographs, etc.</td>
</tr>
<tr>
<td>Acquire the evidence</td>
<td>Collect and preserve the original data, and create an exact copy</td>
</tr>
<tr>
<td>Authenticate the copy</td>
<td>Verify that the copy is identical to the original</td>
</tr>
</tbody>
</table>

(Continued)
## Investigation Objectives & Chain of Custody Practices

<table>
<thead>
<tr>
<th>Investigation Objectives</th>
<th>Chain of Custody Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyze and filter the evidence</td>
<td>Perform the technical analysis while retaining its integrity</td>
</tr>
<tr>
<td>Be objective and unbiased</td>
<td>Ensure that the evaluation is fair and impartial to the person or people being investigated</td>
</tr>
<tr>
<td>Present the evidence/evaluation in a legally acceptable manner</td>
<td>Interpret and report the results correctly</td>
</tr>
</tbody>
</table>
Document and Collect Data

- Documentation needs to be precise and organized

- Document each of the following:
  - Location, date, time, witnesses
  - System information, including manufacturer, serial number, model, and components
  - Status of the computer, such as whether it was running and what was connected to it
  - Physical evidence collected
Power Down or Unplug?

- If a PC is running, the decision has to be made as to how to power it down
  - Using the operating system to power down is risky because temporary files might be deleted and date/time stamps changed
- Current best practice is to unplug the PC from its power source, preserving the data environment
- Is this Correct Practice?
Exceptions to the “Copy Rule”

- Best practice is to work with a copy of the original data
- Exceptions to this rule may occur when it is more important to contain an attack or stop a crime
- It may also be impossible to copy an entire system
In Practice: Write Blocking and Protection

- Never turn on a PC without having write-blocking software or devices in place.
- Write-blocking devices prevent any writes to a drive such as may occur when simply turning on a system.
- What about Flash Drives?
- What about Network Drives?
- What about Memory?
Creating a Drive Image

- Original data must be protected from any type of alteration
- To protect original data, work from a forensic copy of the original drive or device
- Ways to make forensic copies
  - Drive imaging or mirror imaging
  - Sector-by-sector or bit-stream imaging
- Is This Enough?
Residual Data

- Residual data is data that has been deleted but not erased
- Residual data may be found in unallocated storage or file slack space
- File slack consists of:
  - RAM slack—area from the end of a file to the end of the sector
  - Drive slack—additional sectors needed to fill a cluster

- How can we Wipe a disk?
Acquiring a Forensic Copy

- Use a forensically clean hard drive for copying
  - Simple format does not meet acceptable or best practices
- Verify the accuracy of the copy
  - Cyclic redundancy check
  - Cryptographic hash verification
  - Message digest (MD5)
Identify Data Types

- Active data
- Deleted files
- Hidden, encrypted, and password-protected files
- Automatically stored data
- E-mail and instant messages
- Background information
Investigative Environments and Analysis Modes

- **Trusted environments**
  - Dead analysis or postmortem analysis
  - Nonvolatile data or persistent data

- **Untrusted environments**
  - Live analysis
  - Includes both Network and Host Analysis
Forensic Tools and Toolkits

- Tools support the investigator by helping to:
  - Recreate a specific chain of events or sequence of user activities
  - Search for key words and dates and determine which of the data is relevant
  - Search for copies of previous document drafts
  - Search for potentially privileged information
  - Search for the existence of certain programs
  - Authenticate data files and their date and time stamps
Forensic Tools and Toolkits (Cont.)

- **EnCase® Forensic (see DoJ Guide on course site)**
  - A DOD-approved tool for gathering and evaluating electronic information
  - Supports the following e-mail investigation file types:
    - MSN Hotmail
    - Outlook and Outlook Express
    - Yahoo!
    - AOL 6, 7, 8, and 9
    - Netscape
    - mBox (Unix)
Forensic Tools and Toolkits (Cont.)

- EnCase Cybercrime Arsenal is a customizable package of software, hardware, and training
  - Available in three packaged solutions
  - Offers four views of collected data:
    - Table view displays files in a spreadsheet-style format
    - Gallery view provides a view of all images
    - Timeline view provides a calendar-style picture of file activity
    - Report view helps create tailored reports
Other toolkits for Windows:

- Forensic Toolkit® (FTK™)—used for finding and examining computer evidence
- Ultimate Toolkit™—contains FTK plus other modules for recovering passwords, analyzing registry data, and wiping hard drives
- WinHex—used for forensics, data recovery and processing, and IT security
Forensic Tools and Toolkits (Cont.)

- Toolkits for UNIX and Linux:
  - Autopsy and Sleuth Kit—for investigating file systems and volumes of suspect computers
  - dtSearch—for combing through large amounts of data for up to 250 different file types
Macintosh forensic software:
- BlackBag—a set of 19 tools for examining Macintosh computers, including
  - Directory Scan
  - FileSpy
  - HeaderBuilder
- MacQuisition—forensic acquisition tool used to safely image Macintosh systems
Forensic Tools and Toolkits (Cont.)

- **PDA Seizure**
  - A comprehensive forensic tool from Paraben for investigating Palm, Pocket PCs, and BlackBerry devices
  - Can produce forensic images and perform data searches as well as crack passwords for Palm

- **Mobile & Smart-Phone tools**
  - There are a few out there, most recent prototypes
  - We will discuss more during class.
## Forensics Equipment (Cont.)

<table>
<thead>
<tr>
<th>Type</th>
<th>Tool or Toolkit</th>
<th>Free Demo</th>
<th>Web Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password cracker</td>
<td>Passware kit</td>
<td>Yes</td>
<td><a href="http://www.lostpassword.com/kit.htm">www.lostpassword.com/kit.htm</a></td>
</tr>
<tr>
<td>Password cracker</td>
<td>John the Ripper</td>
<td>Yes</td>
<td><a href="http://www.openwall.com/john">www.openwall.com/john</a></td>
</tr>
<tr>
<td>Portable hard disk duplicator</td>
<td>Disk Jockey</td>
<td></td>
<td><a href="http://www.diskology.com">www.diskology.com</a></td>
</tr>
<tr>
<td>Portable hard drive and media duplicator</td>
<td>Logicube</td>
<td></td>
<td><a href="http://www.logicube.com">www.logicube.com</a></td>
</tr>
<tr>
<td>Forensic intrusion detection, and scanning tools</td>
<td>Foundstone</td>
<td>Yes</td>
<td><a href="http://www.foundstone.com/resources/forensics.htm">www.foundstone.com/resources/forensics.htm</a></td>
</tr>
</tbody>
</table>
Certification and Training Programs

- EnCE®—EnCase Certified Examiner
- Global Information Assurance Certification (GIAC)
- Computer Hacking Forensic Investigator (CHFI)
- Computer Forensic External Certification (CCE)
Certification and Training Programs (Cont.)

- TruSecure ICSA Certified Security Associate
- Computer Forensic Training Center Online
- Certified International Information Systems Forensics Investigator (CIFI)
Quality of e-evidence depends on skilled investigators
Maintaining the integrity of e-evidence requires a defensible approach
There can be no weak links in the investigative process
It is vital for the investigator to be able to extract and analyze data quickly and present the evidence in an understandable format
Investigators frequently have to defend their findings, methods, tools, and techniques

Technologies and methodologies must be well documented and repeatable

Specialized software and hardware tools are needed for documentation, collection, authentication, analysis, preservation, and production and reporting of findings and e-evidence
There are several certification and training programs that computer forensics investigators can complete to help them become credible in the field.