The ABC’s of Computer Crimes’ Forensics

Rick Lavaty, Computer Systems Administrator
Computer Forensics . . .
A Defense Prospective

Rick Lavaty
Supervisory Computer Systems Administrator
Federal Public Defender’s Office, AZ
What’s computer forensics?

- Securing and collecting data without compromising the evidence
- Examination and analysis of data by persons with proper experience and training
- Document and preserve the seizure, examination, storage & transfer of data
- Working with attorneys and paralegals to develop electronic disclosure and discovery strategies
- Consulting on computer technology and infrastructure issues in litigation
- Testifying as an independent expert
When do you need one?

- Fraud
- Identity Theft
- Intellectual Property Theft
- Child Pornography
- Stalking/Cyberstalking
Will my expert be expensive?

Oh HELL YES!

What influences costs?
  Time needed for the exam?
  What do you need to know?
  What kind of equipment is needed?
  How fast do you need a report?
  Theory of defense?
  Is it a Child Pornography Case?
Do you really need an expert?

Yeah – You do - unless this looks familiar
Working With an Expert

- Ensure that your expert knows both your client’s and the adverse party’s position, and has seen ALL disclosure.
- Don’t project a bias onto your expert; you want the good news and the bad news.
- Give your expert the access needed to direct an investigation, avoid surprises, and form a valid and supportable opinion.
- Give your expert the time needed from you to prepare for depositions and trial.
- Don’t place unrealistic time constraints on your expert – this can be VERY slow and tedious work.
The Enormous Amount of Data

1 MB of data = 312 pages

20 MB hard drive = 32 inch stack

1.2 GB hard drive = 160 foot stack

80 GB hard drive = 10,000 foot stack
What does L.E. look for?

“Unlike some traditional forensic analyses that attempt to gather as much information as possible from an evidence sample, computer forensic analysis attempts to recover only probative information from a large volume of generally heterogeneous information.”

U.S. Department of Justice - Forensic Science Communications
October 2000  Volume 2  Number 4

Recovering and Examining
Computer Forensic Evidence
WHERE IS THE EVIDENCE?

... and how did it get there?
Here’s some of the places we find it
What We Know – Before Forensic Exam

- Facts surrounding the crime
- Seizure (and acquisition) dates and times
- Type of media (HDD, Cell Phone, Camera)
- Specifications of media (Size, OS, Users, Time Zone)
- Registration information and user accounts
- Folder structure and file listing
- Whether the data is active or deleted
- Where the chargeable evidence exists (sometimes)
What We Don’t Know

• Was the electronic evidence properly handled?
• What evidence of the crime exists on the media, if any? (Probable Cause)
• Where does ALL of the electronic evidence exist? (Not just the evidence the prosecution noted)
• How did it get there?
• When was it created? Accessed? Deleted?
• Was it moved, copied, saved, viewed?
• Who had access to the evidence?
Chapter 3. Evidence Acquisition

Principle: Digital evidence, by its very nature, is fragile and can be altered, damaged, or destroyed by improper handling or examination. For these reasons special precautions should be taken to preserve this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion.
Technical reasons to exclude?

What’s really on that hard drive?

- Viruses, Backdoors & Trojans?
- File access dates and times – How reliable are they?
- How many images?
- .lnk files – did your client access/view it?
- Wi-Fi Home Network?
- P2P File Sharing programs?
- Drive properly handled after seizure?
Who Had Access?

- Computer name - user accounts
- Online User names and passwords (Registry)
- On-line activity and personal data
- Wireless network?? Secure??
- Malware
- Remote Access
DATE / TIME STAMP ANALYSIS

• Last Written (Modified) – date/time when the file was last opened, edited and saved.

• Last Accessed – date/time the file was last touched (This is turned off in Vista & Win 7)

• File Created – date/time the file was created at that location on the media
When the Last Written date/time is equal to the File Created date/time, the file has not been modified or copied from another location.
DATE / TIME STAMP ANALYSIS

• When Last Written date/time is prior to the File Created date/time, the file has been copied or moved from one location to another location.
DATE / TIME STAMP ANALYSIS

• When a group of files is copied or moved, the File Created dates/times will be in sequence with very close and/or identical date/time stamps.
What can be found?

• If the client saw it
  . . A forensic expert can probably find it
• Internet sites
• Saved files
• User names, passwords, and IDs
• Deleted files
• Temp Files
• E-Mail
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>url1</td>
<td>REG_SZ</td>
<td><a href="http://yahoo.com/">http://yahoo.com/</a></td>
</tr>
<tr>
<td>url2</td>
<td>REG_SZ</td>
<td><a href="http://google.com/">http://google.com/</a></td>
</tr>
<tr>
<td>url3</td>
<td>REG_SZ</td>
<td><a href="http://www.gyyv.net/catz">http://www.gyyv.net/catz</a></td>
</tr>
<tr>
<td>url4</td>
<td>REG_SZ</td>
<td><a href="http://www.gyyv.net:2095">www.gyyv.net:2095</a></td>
</tr>
<tr>
<td>url5</td>
<td>REG_SZ</td>
<td><a href="http://www.picture.com/">http://www.picture.com/</a></td>
</tr>
<tr>
<td>url6</td>
<td>REG_SZ</td>
<td><a href="http://wachovia.com/">http://wachovia.com/</a></td>
</tr>
<tr>
<td>url7</td>
<td>REG_SZ</td>
<td><a href="http://cendyne.com/">http://cendyne.com/</a></td>
</tr>
<tr>
<td>url8</td>
<td>REG_SZ</td>
<td>usps</td>
</tr>
<tr>
<td>url11</td>
<td>REG_SZ</td>
<td><a href="http://mixer.dnsart.com">http://mixer.dnsart.com</a></td>
</tr>
<tr>
<td>url12</td>
<td>REG_SZ</td>
<td><a href="http://minnegasco.centerpointenergy.com/">http://minnegasco.centerpointenergy.com/</a></td>
</tr>
<tr>
<td>url13</td>
<td>REG_SZ</td>
<td>google</td>
</tr>
<tr>
<td>url14</td>
<td>REG_SZ</td>
<td><a href="http://jcwhitney.com/">http://jcwhitney.com/</a></td>
</tr>
</tbody>
</table>
[10:59:59] Sign In - Microsoft Internet Explorer
[Del]SNOWBOO55@HOTMAIL.COM
MASH4077BOOBOO (·Changed window·)

[15:44:37] Sign in to Yahoo! - Microsoft Internet Explorer
snowboo40 [TAB]
booboo (·Return·)
AOL Instant Messenger (AIM)
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>MRUList</td>
<td>REG_SZ</td>
<td>bdca</td>
</tr>
<tr>
<td>b</td>
<td>REG_SZ</td>
<td>C:\Documents and Settings\michaelf\Desktop\rock.est</td>
</tr>
<tr>
<td>d</td>
<td>REG_SZ</td>
<td>C:\Documents and Settings\michaelf\My Documents\rock.est</td>
</tr>
<tr>
<td>c</td>
<td>REG_SZ</td>
<td>C:\Documents and Settings\michaelf\Desktop\rorck.est</td>
</tr>
<tr>
<td>a</td>
<td>REG_SZ</td>
<td>C:\Documents and Settings\michaelf\Desktop\copyprotection.bmp</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Data</td>
</tr>
<tr>
<td>-------</td>
<td>--------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>File0</td>
<td>REG_SZ</td>
<td>\Video\d\Eva_Grubb.avi</td>
</tr>
<tr>
<td>File1</td>
<td>REG_SZ</td>
<td>\Video\d\smut\sluts005.mpg</td>
</tr>
<tr>
<td>File2</td>
<td>REG_SZ</td>
<td>\Video\d\smut\Chessie06.AVI</td>
</tr>
<tr>
<td>File3</td>
<td>REG_SZ</td>
<td>\Video\d\smut\Chessie05.AVI</td>
</tr>
<tr>
<td>File4</td>
<td>REG_SZ</td>
<td>\Video\d\smut\Chessie04.AVI</td>
</tr>
<tr>
<td>File5</td>
<td>REG_SZ</td>
<td>\Video\d\smut\Chessie03.AVI</td>
</tr>
<tr>
<td>File6</td>
<td>REG_SZ</td>
<td>\Video\d\smut\Chessie02.AVI</td>
</tr>
<tr>
<td>File7</td>
<td>REG_SZ</td>
<td>\Video\d\smut\Chessie01.AVI</td>
</tr>
<tr>
<td>File8</td>
<td>REG_SZ</td>
<td>\Video\d\smut\sluts006.mpg</td>
</tr>
</tbody>
</table>
The L.E. Report Will Probably Say Something Like:
“Computer media was analyzed using standard computer forensics tools. Numerous pornographic images were located on the computer hard-drive. Comparison to hash values confirms that eleven (11) “known” child pornographic images were stored on the subject’s hard-drive.”
The hash is a checksum (numeric representation) that is mathematically generated and uniquely identifies an application, or collection of data. This basically means the fingerprint of the file. Because it is calculated mathematically based on the binary information (1’s and 0’s that represent the content of a file), it can be used to identify a file regardless of the name/date/etc.

–Jerry Grant, ACE, INV FPD NYW
What’s that in English?

- You have a file named fox.wpd. The file contains these words:
- “The quick brown fox jumps over the lazy dog”
- The MD5 Hash Value of this file is this: 9e107d9d372bb6826bd81d3542a419d6
- You change the contents of the file to:
- “The quick brown fox jumps over the lazy cog”
- The MD5 Hash Value of this file is: 1055d3e698d289f2af8663725127bd4b
HASH Example Comparison

D8BB84A520996EB591502D5783DB8ED5

BC4E00038B15305F352D55653310AA6B
Mathematical Hashing

Hashing to Compare File Contents

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLAN.DOC</td>
<td>38138</td>
</tr>
<tr>
<td>MEMO.DOC</td>
<td>38138</td>
</tr>
</tbody>
</table>

Same Data

049817c4ce9e1a257b1bd8839d723a28

Same Mathematical Hash

049817c4ce9e1a257b1bd8839d723a28
Questions??
An Overview of Some Useful On-line Resources
National Institute of Justice

Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors

www.ojp.usdoj.gov/nij/pubs-sum/211314.htm
Digital Evidence and Forensics

Computers are used for committing crime, and, thanks to the burgeoning science of digital evidence forensics, law enforcement now uses computers to fight crime.

Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone, a personal digital assistant (PDA), a CD, and a flash card in a digital camera, among other places. Digital evidence is commonly associated with electronic crime, or e-crime, such as child pornography or credit card fraud. However, digital evidence is now used to prosecute all types of crimes, not just e-crime. For example, suspects’ e-mail or mobile phone files might contain critical evidence regarding their intent, their whereabouts at the time of a crime and their relationship with other suspects. In 2005, for example, a floppy disk led investigators to the BTK serial killer who had eluded police capture since 1974 and claimed the lives of at least 10 victims.

In an effort to fight e-crime and to collect relevant digital evidence for all crimes, law enforcement agencies are incorporating the collection and analysis of digital evidence, also known as computer forensics, into their infrastructure. Law enforcement agencies are challenged by the need to train officers to collect digital evidence and keep up with rapidly evolving technologies such as computer operating systems.

NIJ’s Electronic Crime Program, which includes the Electronic Crime Center of Excellence, supports the development of tools to assist state and local law enforcement in combating e-crime and collect digital evidence. The program has five main focus areas:

Innocent Images

Online Child Pornography/Child Sexual Exploitation Investigations

The Innocent Images National Initiative (INI), a component of FBI's Cyber Crimes Program, is an intelligence driven, proactive, multi-agency investigative operation to combat the proliferation of child pornography/child sexual exploitation (CP/CSES) facilitated by an online computer. The INI provides centralized coordination and analysis of case information that by its very nature is national and international in scope, requiring unprecedented coordination with state, local, and international governments and among FBI field offices and legal attaches.

Today, computer telecommunications have become one of the most prevalent techniques used by pedophiles to share illegal photographic images of minors and to lure children into illicit sexual relationships. The Internet has dramatically increased the access of the pedophile sex offenders to the population they seek to victimize and provides them greater access to a community of people who validate their sexual preferences.

The mission of the INI is to reduce the vulnerability of children to acts of sexual exploitation and abuse which are facilitated through the use of computers; to identify and rescue child victims; to investigate and prosecute sexual predators who use the Internet and other online services to sexually exploit children for personal or financial gain; and to strengthen the capabilities of federal, state, local, and international law enforcement through training programs and investigative assistance.

The History of the Innocent Images National Initiative

While investigating the disappearance of a juvenile in May 1993, FBI special agents and Prince George's County, Maryland, police detectives identified two suspects who had sexually exploited numerous juveniles over a 25-year period. Investigation into these activities determined that adults were routinely utilizing computers to transmit sexually explicit images to minors and in some instances to lure minors into engaging in illicit sexual activity. Further investigation and discussions with experts both within the FBI and in the private sector, revealed that the utilization of computer telecommunications was rapidly becoming one of the most prevalent techniques by which some sex offenders shared pornographic images of minors and identified and recruited children into sexually illicit relationships. In 1995, based on information developed during this investigation, the Innocent Images National Initiative was started to address the illicit activities conducted by users of commercial and private online services and the Internet.

The INI is managed by the Innocent Images Unit within the FBI's Cyber Division at FBI Headquarters in Washington, DC. Innocent Images field supervisors and investigative personnel work closely with the Innocent Images Unit regarding all INI investigative, administrative, policy, and training matters. The INI provides a coordinated FBI response to this nationwide crime problem by collating and analyzing information obtained from all available sources.

Today the FBI's Innocent Images National Initiative focuses on:

- Online organizations, enterprises, and communities that exploit children for profit or personal gain.
- Major distributors of child pornography, such as those who appear to have transmitted a large volume of child pornography via an online computer on several occasions to several other people.
- Producers of child pornography.
- Individuals who travel, or indicate a willingness to travel, for the purpose of engaging in sexual
Recovering and Examining Computer Forensic Evidence

Michael G. Nobleett
Senior Associate
Booz-Allen & Hamilton
Falls Church, Virginia

Mark M. Pollitt
Unit Chief
Computer Analysis and Response Team
Federal Bureau of Investigation
Washington, DC

Lawrence A. Presley
Training Instructor
Forensic Science Training Unit
Cuarto, Virginia

Read about...

Introduction

Computer Forensic Science

Background
Resources for Law Enforcement

The National Center for Missing & Exploited Children is Now Accepting Nominations for the 2011 National Missing and Exploited Children's Awards.

The National Center for Missing & Exploited Children offers law enforcement powerful resources, free of charge, to help investigate cases of missing and sexually exploited children. In cooperation with the U.S. Department of Justice's Office of Juvenile Justice and Delinquency Prevention, and through the support of private sponsors, we provide assistance with:

- **Missing Children Cases**
- **Child Sexual Exploitation Cases**
- **Training and Education**
- **9-1-1 Call Center Program**
- **Links, Lists, and Tools**

Please call our toll-free, 24-hour hotline at 1-800-THE-LOST® for more information or to request any of these services.

**A Proven Track Record**

Since its creation by Congress in 1984, the National Center for Missing & Exploited Children has assisted law enforcement with more than 148,160 missing child cases, resulting in the recovery of more than 132,300 children. Our CyberTipline, a reporting mechanism for child sexual exploitation, has handled more than 628,680 leads.

**Who We Are**

Our people are our value. The National Center for Missing & Exploited Children (NCMEC) brings a team of more than 350 dedicated and highly-trained professionals with access to an extensive network of resources, research, and cutting-edge technologies. NCMEC staff include former, career law enforcement officers with experience at federal, state, and local levels, as well as forensics experts, technologists, analysts, attorneys, and social workers.
Other Useful References and Links

• Forensic Toolkit
  – http://www.accessdata.com

• Encase Forensic
  – http://www.guidancesoftware.com

• Others
  – http://www.digital-detective.co.uk/
Google: “Computer Forensics”