Regional Computer Forensic Laboratory & Digital Forensics

Presented By:
D. Justin Price
FBI - Philadelphia
Computer Analysis Response Team
Objectives
Objectives

- RCFL Program Overview
- PHRCFL Services
- Forensic Capabilities
- Forensic Process
- Career with the FBI
The PHRCFL is a multi-agency partnership of federal, state and local law enforcement agencies engaged in serving the computer forensics needs of several counties within the Greater Philadelphia area.
The PHRCFL is a multi-agency partnership of federal, state and local law enforcement agencies engaged in serving the computer forensics needs of several counties within the Greater Philadelphia area.
The PHRCFL is a multi-agency partnership of federal, state and local law enforcement agencies engaged in serving the computer forensics needs of several counties within the Greater Philadelphia area.
The PHRCFL is a multi-agency partnership of federal, state and local law enforcement agencies engaged in serving the computer forensics needs of several counties within the Greater Philadelphia area.
The PHRCFL is a multi-agency partnership of federal, state and local law enforcement agencies engaged in serving the computer forensics needs of several counties within the Greater Philadelphia area.
The PHRCFL is a multi-agency partnership of federal, state and local law enforcement agencies engaged in serving the computer forensics needs of several counties within the Greater Philadelphia area.
Computer Forensics?
Computer Forensics?

- The scientific examination of digital evidence for the purpose of presenting findings during court proceedings.

- A verifiable and repeatable process that protects the integrity of original evidence and renders it unchanged.
What is Digital Evidence?

- Computers (Desktops, Laptops, Servers …)
  - Windows, Macintosh, Linux
- Removable Media
  - Magnetic Media, Flash Disks, Optical Media, etc.
- PDAs Palm/Windows CE/Blackberry
  - Palm OS, Windows CE and Blackberry
- Cell Phones
- Audio/Visual Systems (i.e. Surveillance)
- Networks
  - Servers, SAN, NAS, etc.
usb sushi
Digital Storage Media

USB Watch Stores Data
Digital Storage Media

USB Watch Stores Data
Digital Storage Media

USB Watch Stores Data
Digital Storage Media

USB Watch Stores Data
Digital Storage Media

USB Watch Stores Data
Digital Storage Media

USB Watch Stores Data
Digital Storage Media

USB Watch Stores Data
Digital Storage Media
Digital Storage Media

The key chain is a wireless device that communicates with the USB device.

If the two devices get separated by more than 2 meters, the hard drive is encrypted.
As a Result:

• Traditional Crimes are producing digital evidence (lots!)
• Cyber Crimes are producing complex digital evidence
• Law enforcement, at all levels are unprepared for “data glut, Information famine”

One solution......
Regional Computer Forensic Laboratory (RCFL)

- A one stop, full service forensic laboratory devoted entirely to the examination of digital evidence in support of criminal investigations
- A unique law enforcement partnership that promotes quality and strengthens computer forensics laboratory capacity
Typical RCFL Organization

Local Executive Board

RCFL Director

Deputy Director

Administrative Support

Examiner

Examiner

Examiner

Examiner

Examiner

Examiner

Examiner

Examiner

Examiner

Examiner

Examiner

Examiner

Examiner

State and local positions
Status of National Program

Map showing locations of programs:
- Portland, OR
- Salt Lake City, UT
- Menlo Park, CA
- San Diego, CA
- Denver, CO
- Kansas City, MO
- Chicago, IL
- Dallas, TX
- Houston, TX
- Louisville, KY
- Dayton, OH
- Buffalo, NY
- Hamilton, NJ
- Philadelphia, PA

Legend:
- Currently in Operation
- Planned for 2005–2006
Why was the program launched?

- Increase the law enforcement’s capability to investigate crimes and detect and prevent acts of terrorism
- Respond to rapidly growing demand for digital forensic examination services
- Enhance the FBI’s support state and local law enforcement
- Combine the talents and resources of law enforcement agencies at all levels
PHRCFL Services Offered

- Digital Forensic Examination
  - All submitted criminal Evidence from service area
  - Assistance to law enforcement agencies

- Warrant Service
  - Consulting and assistance prior to service.
  - On-site evidence examination when needed

- Training
  - Search and Seizure
  - ImageScan
  - Understanding the Forensic Report
Specialization

- **ASCLD**
  - Digital Forensics
    - Computers
    - Audio
    - Video

- **FBI – CART**
  - WinTel (Windows / Intel based)
  - Macintosh
  - Unix / Linux
  - PDA
  - Cell Phones
Examiner Equipment

- **Wintel**
  - Two Dell 690 Precisions
  - MPC Transport 3200 Laptop
  - Logicube Talon Imaging Devices
  - HP Laser Printer
  - Digital Camera
  - Sony Digital Photo Printer
  - Wiebotech RT5 (RAID Box)
  - Wiebotech Forensic Combodocks
  - SCSI Cards and Cables
  - Media Card Readers
  - Various Software Suites
  - Pelican Search Case
  - Reference Library

- **Macintosh**
  - Mac Pro
  - Macbook Pro
  - Various Software Suites
  - Reference Library

- **Linux**
  - Gigabit Switches
  - Gigabit NICs
  - Cables
  - Reference Library

- **PDA**
  - Garmin iQue M4
  - Various PDA Cable Kit
  - Reference Library

- **Cell Phone**
  - SIM Card Readers
  - DataPilot Forensic Cell Phone Kit
  - Reference Library

Each program procures equipment upgrades each year
Types of Investigations

- Terrorism
- Child Pornography
- Homicide
- Violent Crimes
- The Theft or Destruction of Intellectual Property
- Internet Crime
- Fraud
- Public Corruption
- Every Investigation .........
Cases By Priority

1) Terrorism — Neutralize, dismantle, and prevent terrorist acts against American citizens and assets.
2) Counterintelligence — Expose, prevent, and investigate illegal activities on U.S. soil with a focus on keeping weapons of mass destruction and other embargoed technologies from foreign enemies, protecting the secrets of the U.S. intelligence community, protecting the secrets of the U.S. Government and contractors, protecting our nation’s critical national assets; and focusing on countries that pose the greatest threat to the United States.
3) Cybercrimes — Track and trace persons who use the Internet and computers to illegally penetrate business and government computer systems, including stealing trade secrets and intellectual property, trafficking in child pornography, enticing children from the safety of their homes, and infrastructure protection such as computer networks and power grids.
4) Public corruption—Investigate public officials and those acting under the color of law to seek financial gain based on the public’s trust. These acts include embezzlement, voter fraud, subsidy fraud, illegal kickbacks, and bribes committed by government and/or elected officials.
5) Civil rights—Investigate hate crimes, involuntary servitude/slavery, and blocking patients from accessing health clinics.

6) Organized Crime—Investigate and infiltrate entire organizations that are established for the purpose of committing a host of criminal activities for financial gain or territorial control through various means, including threats, intimidation, and collusion.

7) White Collar Crime—Investigate and trace financial transactions that are deliberately deceptive and have the sole purpose of deriving unlawful financial gain at the public’s expense. Corporate fraud can take place in the areas of health care, mortgage lending, identity theft, insurance, telemarketing, and asset forfeiture/money laundering.

8) Major Thefts/Violent Crime—Investigate and prevent crimes against children, such as molestation, kidnappings, and those criminal acts, including homicide, committed by gangs and drug traffickers.
FY06 RCFL Program
Accomplishments at a Glance

- Accepted 4,214 requests for assistance
- Trained 3,262 law enforcement personnel
- Conducted 4,500 digital forensics examinations
- Available to more than 3,500 law enforcement agencies across 11 states
- Participated in 803 search and seizure operations
- Processed 916 terabytes of data
CART Capabilities

• Analyze IBM compatible CPUs, Macintosh, Linux, Unix, optical media, magnetic media, PDAs and cell phones.
• Analyze Servers (Email, Web, File, etc.), RAID Arrays (Hardware and Software), SANs, etc.
• Create a complete file listing of each exhibit with all attributes.
• Recover deleted data.
• Recover deleted partitions.
• Recover data from formatted media.
• Recover text from password protected and/or encrypted documents.
• Disable boot-up passwords.
• Recover text fragments from chat rooms and instant messaging.
• Recover files that have not been saved, but printed or scanned.
• Recover computer’s internet activity.
• Generate a timeline of computer activity.
• Recover Data from Registry (i.e. passwords, recent chats, etc.)
CART Capabilities

- Analyze IBM compatible CPUs, Macintosh, Linux, Unix, optical media, magnetic media, PDAs and cell phones.
- Analyze Servers (Email, Web, File, etc.), RAID Arrays (Hardware and Software), SANs, etc.
- Create a complete file listing of each exhibit with all attributes.
- Recover deleted data.
- Recover deleted partitions.
- Recover data from formatted media.
- Recover text from password protected and/or encrypted documents.
- Disable boot-up passwords.
- Recover text fragments from chat rooms and instant messaging.
- Recover files that have not been saved, but printed or scanned.
- Recover computer’s internet activity.
- Generate a timeline of computer activity.
- Recover Data from Registry (i.e. passwords, recent chats, etc.)
CART Capabilities

- Analyze IBM compatible CPUs, Macintosh, Linux, Unix, optical media, magnetic media, PDAs and cell phones.
- Analyze Servers (Email, Web, File, etc.), RAID Arrays (Hardware and Software), SANs, etc.
- Create a complete file listing of each exhibit with all attributes.
- Recover deleted data.
- Recover deleted partitions.
- Recover data from formatted media.
- Recover text from password protected and/or encrypted documents.
- Disable boot-up passwords.
- Recover text fragments from chat rooms and instant messaging.
- Recover files that have not been saved, but printed or scanned.
- Recover computer’s internet activity.
- Generate a timeline of computer activity.
- Recover Data from Registry (i.e. passwords, recent chats, etc.)
CART Capabilities

- Analyze IBM compatible CPUs, Macintosh, Linux, Unix, optical media, magnetic media, PDAs and cell phones.
- Analyze Servers (Email, Web, File, etc.), RAID Arrays (Hardware and Software), SANs, etc.
- Create a complete file listing of each exhibit with all attributes.
- Recover deleted data.
- Recover deleted partitions.
- Recover data from formatted media.
- Recover text from password protected and/or encrypted documents.
- Disable boot-up passwords.
- Recover text fragments from chat rooms and instant messaging.
- Recover files that have not been saved, but printed or scanned.
- Recover computer’s internet activity.
- Generate a timeline of computer activity.
- Recover Data from Registry (i.e. passwords, recent chats, etc.)
• Often, computers are not in pristine condition when they arrive for examination.

• They are occasionally:
  • Burned
  • Water-logged
  • Shot
  • Dropped
  • Bludgeoned
  • Just such antiques that the technology to retrieve information from them no longer exists.
Where is digital evidence?

- Digital Information in evidence may be:
  - Encrypted
  - Compressed
  - Hidden
  - Deleted
  - In free space
  - Password-protected

- In all cases, attempts must be made to render the information viewable.
<table>
<thead>
<tr>
<th>Name</th>
<th>Attack Type</th>
<th>File Type</th>
<th>Begin Time</th>
<th>End Time</th>
<th>Status</th>
<th>Priority Group</th>
<th>Priority (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Protected Document</td>
<td>Microsoft Word 97/2000 Password Attack</td>
<td>Word</td>
<td>19/02/06 13:19:53</td>
<td>19/02/06 10:20:20</td>
<td>Finished <em>password...</em></td>
<td>Normal</td>
<td>0.00%</td>
</tr>
</tbody>
</table>
### AccessData Distributed Network Attack 3 - Supervisor (localhost)

#### Priority Groups

<table>
<thead>
<tr>
<th>Group</th>
<th>Priority (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>90.00%</td>
</tr>
<tr>
<td>Normal</td>
<td>10.00%</td>
</tr>
<tr>
<td>Waiting</td>
<td></td>
</tr>
<tr>
<td>Finished</td>
<td></td>
</tr>
</tbody>
</table>

#### Workers

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Processors</th>
<th>Connect</th>
<th>Last Contact Time</th>
<th>Working On</th>
<th>Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRECEDING</td>
<td>192.168.1.3</td>
<td>2</td>
<td>Y</td>
<td>10/02/06 10:29:23</td>
<td>Password Protected Document (Microsoft Word 97/2000 Password Attack)</td>
<td>Default</td>
</tr>
<tr>
<td>localhost</td>
<td>127.0.0.1</td>
<td>2</td>
<td>Y</td>
<td>10/02/06 10:29:28</td>
<td>Password Protected Document (Microsoft Word 97/2000 Password Attack)</td>
<td>Default</td>
</tr>
</tbody>
</table>

### File Information

<table>
<thead>
<tr>
<th>Name</th>
<th>Attack Type</th>
<th>File Type</th>
<th>Begin Time</th>
<th>End Time</th>
<th>Status</th>
<th>Priority Group</th>
<th>Priority (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Protected</td>
<td>Microsoft Word 97/2000 Password Attack</td>
<td>Word</td>
<td>10/02/06 10:24:07</td>
<td></td>
<td>Running</td>
<td>Normal</td>
<td>%100.00</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
<td>Number Complete</td>
<td>Size</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>-------------------------------------------------------</td>
<td>-----------------</td>
<td>--------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>Dictionary primary search (EN-1) Common-en-u.adf</td>
<td>0 (0.00%)</td>
<td>8,480</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Dictionary primary search (EN-2) Passwords-en-u.adf</td>
<td>0 (0.00%)</td>
<td>14,228</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Dictionary primary search (EN-3) Crime-en-u.adf</td>
<td>0 (0.00%)</td>
<td>23,242</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Dictionary primary search (EN-4) Miscellaneous-en-u.adf</td>
<td>0 (0.00%)</td>
<td>50,420</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Dictionary primary search (EN-5) Names-en-u.adf</td>
<td>0 (0.00%)</td>
<td>1,493,412</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Dictionary primary search (EN-6) General-1-en-u.adf</td>
<td>0 (0.00%)</td>
<td>1,281,264</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Dictionary primary search (EN-7) General-2-en-u.adf</td>
<td>0 (0.00%)</td>
<td>1,281,264</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Dictionary primary search (EN-8) General-3-en-u.adf</td>
<td>0 (0.00%)</td>
<td>90,920</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Dictionary primary search (EN-9) General-4-en-u.adf</td>
<td>0 (0.00%)</td>
<td>1,403,412</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Dictionary primary reverse search (EN-2) Passwords-en-u.adf</td>
<td>0 (0.00%)</td>
<td>14,228</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Dictionary primary reverse search (EN-3) Crime-en-u.adf</td>
<td>0 (0.00%)</td>
<td>23,242</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Dictionary primary reverse search (EN-4) Miscellaneous-en-u.adf</td>
<td>0 (0.00%)</td>
<td>50,420</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Dictionary primary reverse search (EN-5) Names-en-u.adf</td>
<td>0 (0.00%)</td>
<td>1,493,412</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Dictionary primary reverse search (EN-6) General-1-en-u.adf</td>
<td>0 (0.00%)</td>
<td>1,281,264</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Dictionary primary reverse search (EN-7) General-2-en-u.adf</td>
<td>0 (0.00%)</td>
<td>1,281,264</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Dictionary primary reverse search (EN-8) General-3-en-u.adf</td>
<td>0 (0.00%)</td>
<td>90,920</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Dictionary primary reverse search (EN-9) General-4-en-u.adf</td>
<td>0 (0.00%)</td>
<td>1,403,412</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Dictionary primary followed by one digit search (EN-1) Common-en-u.adf</td>
<td>0 (0.00%)</td>
<td>84,800</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Dictionary primary followed by one digit search (EN-2) Passwords-en-u.adf</td>
<td>0 (0.00%)</td>
<td>192,280</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Dictionary primary followed by one digit search (EN-3) Crime-en-u.adf</td>
<td>0 (0.00%)</td>
<td>234,200</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Dictionary primary followed by one digit search (EN-4) Miscellaneous-en-u.adf</td>
<td>0 (0.00%)</td>
<td>909,200</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Dictionary primary followed by one digit search (EN-5) Names-en-u.adf</td>
<td>0 (0.00%)</td>
<td>1,493,412</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Dictionary primary followed by one digit search (EN-6) General-1-en-u.adf</td>
<td>0 (0.00%)</td>
<td>1,281,264</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Dictionary primary followed by one digit search (EN-7) General-2-en-u.adf</td>
<td>0 (0.00%)</td>
<td>1,281,264</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Dictionary primary followed by one digit search (EN-8) General-3-en-u.adf</td>
<td>0 (0.00%)</td>
<td>90,920</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Dictionary primary followed by one digit search (EN-9) General-4-en-u.adf</td>
<td>0 (0.00%)</td>
<td>1,403,412</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Level Progress**

![Level Progress Graph](image)
What is the Process?

- With legal authority, evidence is seized
- Evidence is collected and a chain of custody begins
- The case investigator requests an examination for certain (relevant) items
- It is admitted into the Laboratory and documented by barcode, photograph and markings.
- It is prioritized and assigned to an Examiner
- The Examiner further photographs and marks the evidence to ensure uniqueness
- Protocols are followed to ensure that the digital evidence is unchanged and an archive image is made.
- Subsequent examination is of the archive image, not the original evidence unless otherwise unfeasible.
Protecting the Original Evidence

- Hardware Write-Blocking Devices
  - Logicube Talon Device
  - Wiebtech Forensic ComboDock
  - A-Card

- Software Write-Blocking Devices
  - Linux (Mounting Read-Only)
  - Windows Write-Blocking Software (In-House Product)
Protecting the Original Evidence

- **Hardware Write-Blocking Devices**
  - Logicube Talon Device
  - Wiebetechn Forensic ComboDock
  - A-Card
- **Software Write-Blocking Devices**
  - Linux (Mounting Read-Only)
  - Windows Write-Blocking Software (In-House Product)
Protecting the Original Evidence

- Hardware Write-Blocking Devices
  - Logicube Talon Device
  - Wiebetech Forensic ComboDock
  - A-Card
- Software Write-Blocking Devices
  - Linux (Mounting Read-Only)
  - Windows Write-Blocking Software
    (In-House Product)
How is digital media copied?

• All tools has been tested and verified by the FBI. All tools create a low level bit-by-bit copy of the original physical device.

• Forensic suites use the MD5 and/or SHA2 algorithm to verify the image’s authenticity.

• Physical Devices
  • Logicube

• Software Devices
  • Linux DD command
  • EnCase
  • Forensic Tool Kit (FTK)
Imaging in the Laboratory

SAN

Hard Drives

External Hard Drives

HP Ultrium 960
On-Site Imaging

Mobile SAN

Wiebotech RT5

RAID Falcon
Hardware, software, programs, techniques, and skills are employed to uncover and render viewable any relevant information from the device:

- E-Mail messages are made viewable
- Deleted files are restored
- File remnants in slack are “carved” and restored
- Compressed files are opened and examined
- Passworded files are bypassed and made viewable
- Encrypted files are identified and broken in most cases
- Steganographic files are identified
- Databases are reconstructed and made workable
- Other things happen depending on need…

Meticulous notes are kept so that each step could be repeated by another examiner to get the same result.
A file listing, logs, and relevant files are copied to an unalterable media, usually CD-R or DVD-R as archive.

A report of the examination process and the contents of the report media (CD-R or DVD-R) is made.

The case file is submitted to another Examiner for Peer Review to ensure that all protocols were followed and that the report matches what was requested.

The case is returned to the Examiner and then submitted to the Laboratory Director for Administrative Review.

Once all reviews are satisfied, the case investigator is notified to pick up the report and evidence from the Lab.

The chain of custody, reports, report media, notes, receipts, legal authority and logs are archived.
A Career with the FBI

- Visit www.fbijobs.com for all jobs postings
- CART positions are posted as “IT Specialist (Forensic Examiner) – GS 11/12/13 ($57,845 to $107,185)
- All applicants must have a baccalaureate degree with at least 20 semester hours in one or more of the following disciplines: computer science, information systems analysis, science/technology, information management, mathematics, computer engineering, or electrical/electronic engineering.
- Must pass (survive) intensive background investigation for TS level clearance.
Contact Information
Contact Information

D. Justin Price
Federal Bureau of Investigation
Computer Analysis Response Team
201 King of Prussia Road, Suite 300
Radnor, PA 19087
610-975-5125
dprice@rcfl.gov

QUESTIONS??