Computer Forensic Capabilities
Agenda

• What is computer forensics?
• Where to find computer evidence
• Forensic imaging
• Forensic analysis
What is “Computer Forensics”?

- The preservation, identification, extraction, analysis, and interpretation of digital data, with the expectation that the findings will be introduced in a court of law.
Capabilities

• Reveals direct evidence on the machine
• Associates a machine with data
• Provides investigative leads
• Reveals evidence that corroborates or refutes allegations or alibis
• Reveals behavioral evidence
Case Agent-Examiner Relationship

• The case agent and forensic examiner must work as a team

• Case agent
  – Involves examiner early
  – Explains case
  – Provides focused requests

• Forensic examiner
  – Educates and advises investigator
  – Explains results and limitations
Where to Find Computer Evidence

- Seize items specified in the search warrant:
  - Computers, laptops, Network Equipment (hubs and switches)
  - Peripherals: CDR’s, DVD-R’s, Digital cameras, PDA’s
  - External Media: CD’s, floppy disks, USB thumb drives
  - Paper notes, documentation and manuals, post-it notes
- Document computer equipment and peripherals prior to removal:
  - Digital pictures, diagrams
Types of Electronic Media

- Desktops to Servers
Variety of Media
But Wait, There’s More
What is Forensic Imaging?

- Obtained by a method which does not, in any way, alter any data on the drive being duplicated.
- Duplicate must contain a copy of every bit, byte and sector of the source drive.
- Duplicate will not contain any data except filler characters (for bad areas of the media) other than that which was copied from the source media.
- Accurate, Verifiable, Reproducible.
Value of Forensic Imaging

• Incident Response/Forensic Imaging is the MOST IMPORTANT step in the entire electronic investigation

• Failure can invalidate or make inadmissible all further information gathered from the digital evidence
  – Or at least give attorneys a headache
The Imaging Process

010011
010101
01

010011
010101
01

WriteBlock

Imaging
Hardware
or
Software

Hardware
Physical Write Blocks

• What Are They?
  – Physical device that prevents writes to the evidence drive
  – BEST method of imaging
Attaching Write Block
Attaching Write Block
Hardware Imager

Suspect Drive

Forensic Drive
Software Imaging

- Bootable CDs or floppies
- Control computer so it only issues read commands to the drive, never write
- Examples:
  - FTK Imager
  - EnCase
  - DD
  - Ghost
  - Others
Physical vs. Logical

- Physical data structure refers to the actual organization of data on a storage device. Physical imaging gets all the zeros and ones possible from the device.

- Logical data structure refers to how the information appears to a program or user as seen through the operating system. Logical imaging misses data from areas not seen by the operating system.
PROCESS OVERVIEW
What Can the Examiner Find?

- Deleted files
- Text fragments
- Enhanced metafiles (previously printed files)
- Enhanced metadata (embedded information)
- Date/time stamp information
- E-mail messages and chat logs
- Internet usage information (history)
- Archived and compressed files (zip)
- Encoded e-mail attachments
- Images (active and deleted)

AND MORE...
Forensic Request from Case Agent

• EXAMPLE: Kidnapping assault of Heather Miller
  – Evidence of defendant’s involvement with abduction
  – Search for victim’s name
  – Pictures of victim
  – Evidence of threatening letter sent to victim
  – Evidence of references to date rape drugs
  – Evidence of conspirator
  – Activity on the computer during time of crime
  – User attribution

Key word searches
Getting Started

• Keyword Searches
• Drawbacks to key word searches
  – Adobe PDF documents
  – Faxes
  – Excel
  – Registry
  – Compound/Compressed Files
  – Several others
• Right now we have the Victim’s name “Heather Miller” and we know what she looks like. What do you want to do first?
• Key word search for victim’s name reveals no relevant Information.
• Next: review graphics
Graphics Review
Graphics Review

Email with attachment
Subject: pics from last weekend
From: Maryland Dirdbag
Date: 2/20/2007 1:22:41 PM
To: pswift2007@gmail.com

Buddy, here is the pics from last weekend. I felt like a king on presidents holiday.

>From: "Peter Swift" <pswift2007@gmail.com>
>To: <mdhosebag@hotmail.com>
>Subject: last one
>Date: Thu, 15 Feb 2007 14:53:26 -0500
>
>this is the last one for a bit, you should be able to get you jollies from
>
Email Headers

Standard Header Information
Delivered-To: pswift2007@gmail.com
Received: by 10.64.153.3 with SMTP id a3cs152336qbe;
    Tue, 20 Feb 2007 10:22:41 -0800 (PST)
Received: by 10.114.126.1 with SMTP id y1mr3442785wac.1171995758192;
    Tue, 20 Feb 2007 10:22:38 -0800 (PST)

Tue, 20 Feb 2007 10:21:38 -0800
Message-ID: <BAY115-F286B576945D5DB4E9F0288B3890@phx.gbl>
Received: from 65.54.250.200 by by115fd.bay115.hotmail.msn.com with HTTP;
    Tue, 20 Feb 2007 18:21:36 GMT
X-Originating-IP: [66.166.254.82]
X-Originating-Email: [mdhosebag@hotmail.com]
X-Sender: mdhosebag@hotmail.com
From: "Maryland Dirtbag" <mdhosebag@hotmail.com>
To: pswift2007@gmail.com
Bcc:
Subject: pics from last weekend
Date: Tue, 20 Feb 2007 13:21:36 -0500
Mime-Version: 1.0
Content-Type: multipart/mixed; boundary="-----_NextPart_000_1290_1f21_3b10"
X-OriginalArrivalTime: 20 Feb 2007 18:21:38.0744 (UTC) FILETIME=[F6436B80:01C7551B]
Return-Path: mdhosebag@hotmail.com

Time Analysis
Types of Email Metadata

• What types of Metadata are available
  – When Created
  – How Created
  – When Sent
  – When Received
  – Who Sent/Received
  – Route

– Time Analysis
– Graphic Analysis
– Origination
– Who Created it
– When Created
– Application Logs
Reply Email

Subject: RE: pics from last weekend
From: Peter Swift
Date: 2/20/2007 1:29:00 PM
To: Maryland Dirtbag

Thank!

Original Message:

From: Maryland Dirtbag [mailto:mdhosebag@hotmail.com]
Sent: Tuesday, February 20, 2007 1:22 PM
To: pswift2007@gmail.com
Subject: pics from last weekend
Internet Cache-Copy of “Message005”

From: Peter Swift

Subject: last one

Date: Thu, 15 Feb 2007 14:50-0500

To: mdhosebag@hotmail.com

Buddy, here is the pics from last weekend. I felt like a king on presidents holiday.

On 2/20/07, Maryland Dirtbag <mdhosebag@hotmail.com> wrote:

On 2/20/07, <br class="v-line">claydon3@gmail.com> Maryland Dirtbag<br>

I'll talk more later.

---

Chat logs in time analysis
Chat Logs

Session Start: Friday, February 16, 2007
Participants:
  Peter (pswift2007@hotmail.com)
  Maryland (mdhosebag@hotmail.com)

[03:11:39 PM] Maryland: pics not doing it for me anymore.
[03:11:48 PM] Peter: i know what you mean
[03:12:09 PM] Maryland: I found a suitable replacement
[03:12:12 PM] Peter: What are you thinking about
[03:12:29 PM] Maryland: you remember the drugged up mom I was telling you about?
[03:12:45 PM] Peter: Yeah? What do you have in mind?
[03:13:22 PM] Maryland: How about creating some pics of our own?
[03:13:30 PM] Peter: cool. how
[03:14:33 PM] Maryland: Daughter is at the bus stop every day at 3PM
[03:14:40 PM] Peter: yeah
[03:15:08 PM] Maryland: we “invite” her to our clubhouse.
[03:15:26 PM] Maryland: Then let the fun begin...
[03:15:31 PM] Peter: Nice, count me in
[03:15:35 PM] Peter: when?
[03:15:52 PM] Maryland: meet me sat at 2PM at the Exxon near the school.
[03:16:11 PM] Maryland: bring your digital camera, I have all the rest.
[03:16:19 PM] Peter: sweet
[03:16:25 PM] Peter: see ya at 2
Joy.zip

• Metadata from Joy.zip

How are we going to search for this? Keyword
### Time Analysis

#### File List:

<table>
<thead>
<tr>
<th>File Path</th>
<th>File Name</th>
<th>R.</th>
<th>Cr Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>\Documents and Settings\spike\Local Settings\History\His...</td>
<td>MSHist0120070220200...</td>
<td></td>
<td>2/20/2007 1:22:10 PM</td>
</tr>
<tr>
<td>\Documents and Settings\spike\Local Settings\Application...</td>
<td>Message0005</td>
<td></td>
<td>2/20/2007 1:24:27 PM</td>
</tr>
<tr>
<td>\Documents and Settings\spike\Recent\Joy.zip.Ink</td>
<td>Joy.zip.Ink</td>
<td></td>
<td>2/20/2007 1:25:27 PM</td>
</tr>
<tr>
<td>\my joy\Thumbs.db\encryptable</td>
<td>encryptable</td>
<td></td>
<td>2/20/2007 1:26:55 PM</td>
</tr>
<tr>
<td>\my joy\Thumbs.db</td>
<td>Thumbs.db</td>
<td></td>
<td>2/20/2007 1:26:55 PM</td>
</tr>
<tr>
<td>\my joy\back yard fun\Thumbs.db\encryptable</td>
<td>encryptable</td>
<td></td>
<td>2/20/2007 1:26:56 PM</td>
</tr>
<tr>
<td>\my joy\back yard fun\Thumbs.db</td>
<td>Thumbs.db</td>
<td></td>
<td>2/20/2007 1:26:56 PM</td>
</tr>
<tr>
<td>\Documents and Settings\spike\Local Settings\Application...</td>
<td>Message0006</td>
<td></td>
<td>2/20/2007 1:27:40 PM</td>
</tr>
<tr>
<td>\Documents and Settings\spike\Local Settings\Temporary...</td>
<td>21342DD7F237E3C2D...</td>
<td></td>
<td>2/20/2007 1:30:25 PM</td>
</tr>
</tbody>
</table>

#### Highlighted:

- 7 Highlighted

---

**Link File w/Thumb drive**
What does this tell us?

TRANSCEND?
What is “Transcend”?
Google is Your Friend
Google is Your Friend (Images)

Next we find a LINK file...
Web History

- Identify web surfing session
  - Where/when did they open browser?
  - How did they get to the significant finding?
  - Web mail
  - Other Activities?
- All goes toward user attribution
Summary

• Electronic evidence is everywhere
• Case agents must work closely with examiners
• Forensic examiners must look beyond the “Single File”
• Metadata can be critical to establishing user attribution
• Even if evidence itself has been deleted/destruction, numerous artifacts can be found