Autopsy 3.0
Extensible Desktop Digital Forensics
It’s not your father’s open source software

Brian Carrier
VP of Digital Forensics
Basis Technology
Quick Intro To Basis Technology

• Software and services technology company
• Roughly 80 people
• Offices in Cambridge, DC, Tokyo, and London
• Two technology areas:
  – Text Analytics
  – Digital Forensics
Digital Forensics at Basis

- Conduct investigations
- Research and development
- Custom software development
- Open Source Software
  - Autopsy module development
  - Commercial support
  - Training
Open Source Software

• What comes to your mind first?
• What comes to your mind first?

• Autopsy 3 is different
• Open source software that allows you to forensically analyze disk images and local drives
• Original method for using TSK
• Over 25 different tools (!)
• mmls example:

```
# mmls tsk1.img

<table>
<thead>
<tr>
<th>Slot</th>
<th>Start</th>
<th>End</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:</td>
<td>-----</td>
<td>0000000</td>
<td>0000000</td>
<td>0000001</td>
</tr>
<tr>
<td>01:</td>
<td>-----</td>
<td>0000001</td>
<td>0000062</td>
<td>0000062</td>
</tr>
<tr>
<td>02:</td>
<td>00:00</td>
<td>0000063</td>
<td>0032129</td>
<td>0032067</td>
</tr>
<tr>
<td>03:</td>
<td>00:01</td>
<td>0032130</td>
<td>0064259</td>
<td>0032130</td>
</tr>
</tbody>
</table>
```

© 2013, Basis Technology
• Software libraries allow functionality to be embedded in a bigger program.
• Many commercial, open source, and gov'n’t systems use TSK as a library.
• Looks like:

tsk_img_open(1, “C:\imgs\image1.E01”, TSK_IMG_TYPE_DETECT, 512);
Talk to me after if you are building a system that needs this.
• Powerful volume and file system analysis tools.
• Extensible framework.
• Not user friendly for the 99%.
Autopsy

• Graphical digital forensics interface.
• Brief History:
  – 2001: First Open Source Release
    • Interface to The Sleuth Kit
    • Linux and OS X only
  – 2010: Started v3 from scratch as a platform
    • Based on OSDFCon discussions
    • Windows-based & automated
    • Some US Army funding (with 42Six Solutions)
    • 3.0.0 released in September, 2012.
Autopsy 3 Key Points

- Extensible
  - Several frameworks and plug-in modules
- Easy to use
  - Simple UI concepts
  - More details during the demo
- Fast results
  - Provided as soon as they are found
- Cost Effective
  - Free
Autopsy Ingest Modules

Run automatically as media is added to Case.

- Remembers what you ran last time.
- Anyone can write new modules.
- Can tweak knobs based on investigation type and available time.
• Hash Lookup:
  – NSRL, EnCase, Hashkeeper support
• Keyword Search:
  – Lucene SOLR index
  – Extract text (better for HTML and PDF)
  – Import / export lists
  – Regular expressions
  – Can support more advanced text analytics
Recent Activity Module:
  – Browser artifacts:
    • History, cookies, downloads, bookmarks
    • Firefox, Chrome, Safari, IE
  – Recent user documents
  – Recent devices
  – Runs regrripper behind the scenes
• EXIF from JPEGs
• MBOX email
• ZIP Archive
Future Ingest Module Ideas

- More file formats / P2P logs
- Anti-virus / Malware
- Volume shadow / file system journals
- Cryptography and steganography detection
- Text analytics (language detection)
- Object identification in pictures
- Skin tone detection
Content Viewer Modules

• Display a file in a given way.
• Text: Hex and Strings
• Media: Pictures and video
Content Viewer: Video Triage
• Not part of open source package
• Name finder and translator
  – Uses Basis Technology text analytics
External Viewer Module: Timeline
Demo
Takeaway

• Easy to install and use
  – Less training and confusion.

• Extensible and open
  – Can be adapted to your needs
  – Updated by community

• **Low cost**

• **No cost**
• 4th Annual Open Source Forensics Conference
  – Free for government employees!
  – http://www.osdfcon.org/
  – Nov 4 and 5 in Northern VA.
• Cash prizes for best new module.
  – $1500 for first prize
• Voting by attendees at OSDFCon.
• Any module type is eligible.
• See issue tracker for ideas.
• Submission details:
• 2 Day Autopsy training courses:
  – August 21 & 22 in DC
  – November 6 & 7 in DC (after OSDFCon)
• ½ Day Developer Training at OSDFCon
What You Can Do

• Users:
  – Use it and spread the word
  – Provide feedback on features
  – Help with documentation and support
• Developers: Write modules instead of stand-alone apps. Contact us with feature changes.
• We’re looking for law enforcement users.
• Download from:
  – http://www.sleuthkit.org/autopsy/

• Questions: brianc@basistech.com

• We’re hiring engineers....
Demo Highlights
(In Case Demo Fails)
Easy To Use
Splash Screen

- User is always guided to next step in process
Add Image Wizard

- Detects image format
- Detects volume and file systems

Enter Disk Image Information:

- Select input type to add: Image File
- Browse for an image file:
  Z:\vmware-share\autospy-image-v3\image-v3
- Please select the image timezone: (GMT-5:00) America/New_York
- ignore orphan files in FAT file systems
  (faster results, although some data will not be searched)

Press 'Next' to analyze the disk image, extract volume and file system data, and populate a local database.
Ingest Manager in Wizard

- Uses previous settings for modules.
Intuitive Interface

- All results on left, history buttons, keyword search box
Single Place for All Results
View By File Type
View Final Days of Activity
Ingest Inbox

- Shows users what has been found in background tasks
**Report modules can be customized**

**Web History (284)**

<table>
<thead>
<tr>
<th>URL</th>
<th>Date Accessed</th>
<th>Referrer</th>
<th>Name</th>
<th>Program</th>
</tr>
</thead>
</table>
Brian Carrier
Basis Technology
brianc@basistech.com
Desk: 617-386-7132