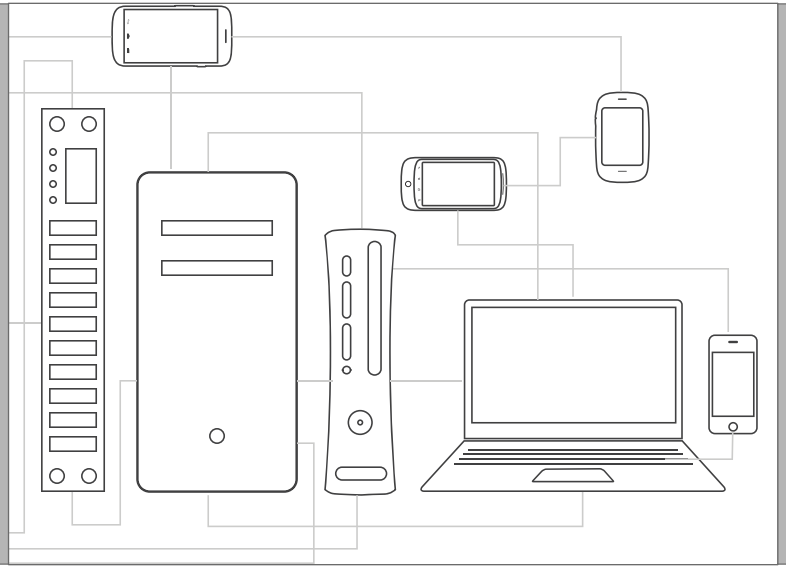
Autopsy® 3: Faster, Better, and still Free



Brian Carrier

BASIS TECHNOLOGY

Agenda

- Part 1: Autopsy essentials
- Part 2: What's new since OSDFCon 2013
- Part 3: What's next

Role Replacement

Role of Hash the Hound is now being played by:

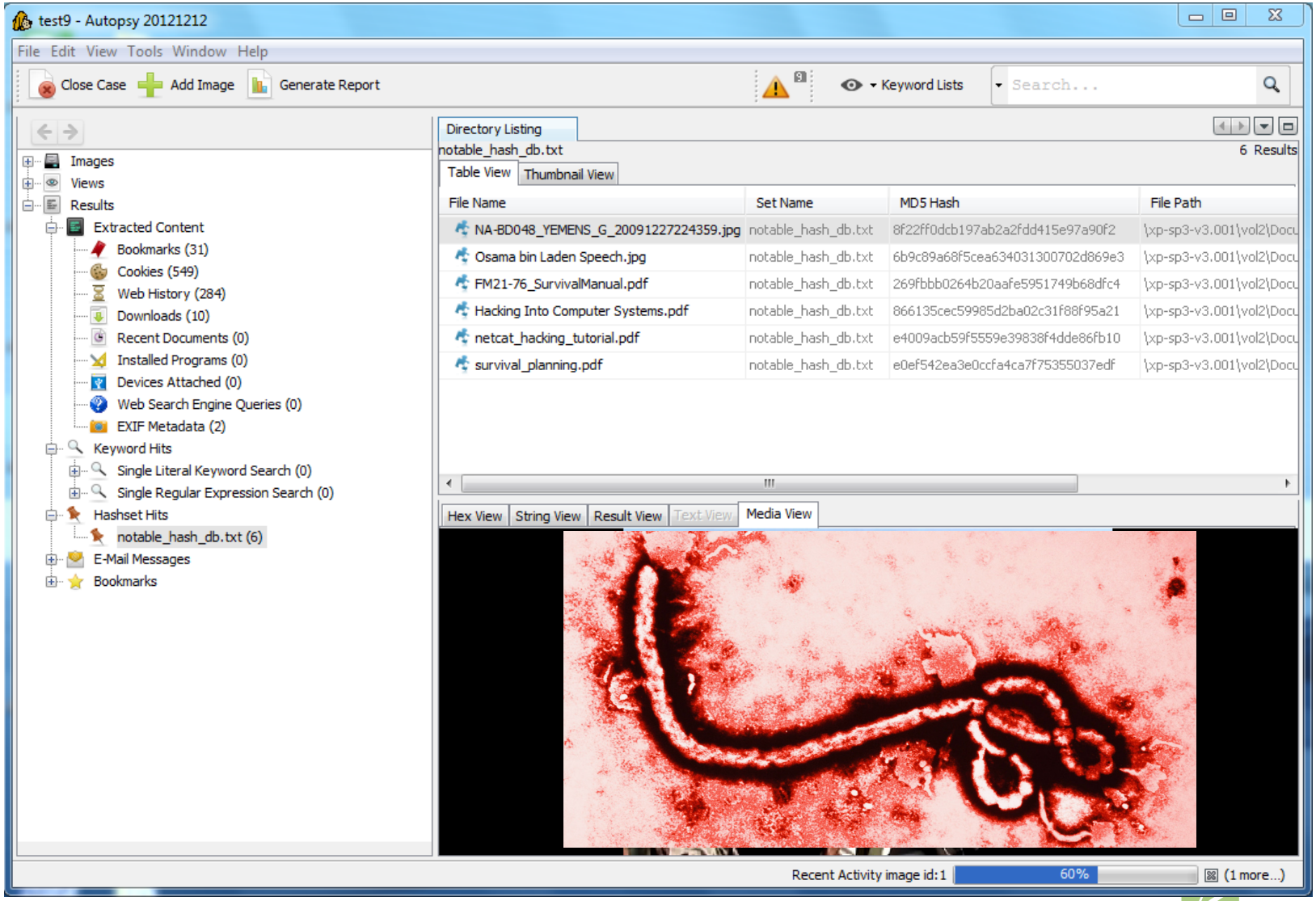
- Slash
- ROT13 the Rottweiler
- Renzix
- ???

Part 1: Autopsy Essentials

What is Autopsy?

- Open Source Digital Forensics Tool
- Focused on Windows (not just Linux)
- Easy to use
- You can use it to:
  - Replace your existing tools
  - Augment your existing tools
  - Validate your existing tools

Autopsy 3 Main Screen



BASIS TECHNOLOGY

Autopsy's 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 2010 discussions
  - Windows-based & automated
  - US Army funding
  - 3.0.0 released in September, 2012.
  - US DHS S&T funding for law enforcement-focused modules.

Key Concepts

- Easy to Use
  - Simple UI concepts
  - All results are in the tree
- Fast Results
  - Provided as soon as they are found
  - Analyze files in parallel on multi-core systems
- Extensible
  - Several frameworks and plug-in modules
- Free

Standard Features

- Standard file systems
- Hash calculation and lookup
- Keyword search (indexed via SOLR)
- Web activity
- Registry (regripper)
- File type and extension mismatch
- Android
- EXIF
- E-mail
- ZIP
- …

Part 2: What's New

Summary

- Lots of new features. Few releases.
  - 3.0.9: February
  - 3.1.0: August
  - 3.1.1: November

- Framework stability is major reason for big gap between 3.0.9 and 3.1.0.
- 18k+ downloads per release (from sf.net).

New Stuff

- New Modules:
  - File type by signature
  - Extension mismatch
  - Interesting Files (flag files based on name patterns)
  - KML Report Module
- Can create Autopsy hash databases
- Localized into Japanese
- ExFAT support (NPS contract)

Android Module

- Extracts:
  - Text, Call logs, Contacts
  - Tango
  - Words With Friends
  - …

- Lots more third-party apps could be supported.
  - Our goal was to show it could be easily done.
- Contributing to this is an easy way to get started.

Python Scripting

- Added in 3.1.1
- Based on Jython
- Long-term request
- Ingest and report modules:
  - Can analyze files based on metadata, content, and output of other modules.
  - Have full access to the database
- See Richard's talk this afternoon for details.

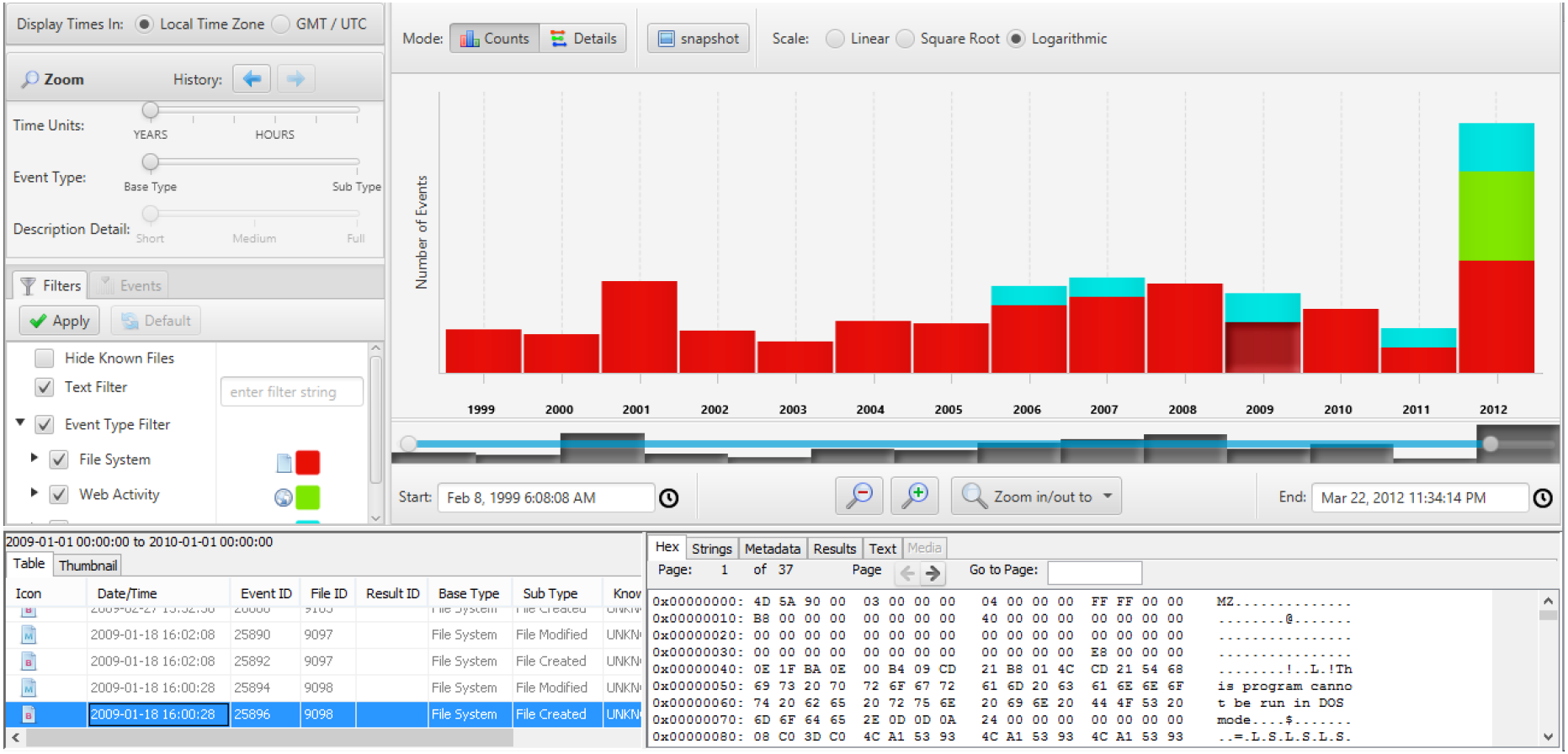
Multi-threaded Pipelines

- 3.0 would analyze only 1 file at a time.
- 3.1 will analyze: 1, 2, 4, 8, etc.
- Takes advantage of multi-core systems
- Sample Image:
  - 7 minutes before
  - 3.5 minutes now

DHS S&T Work

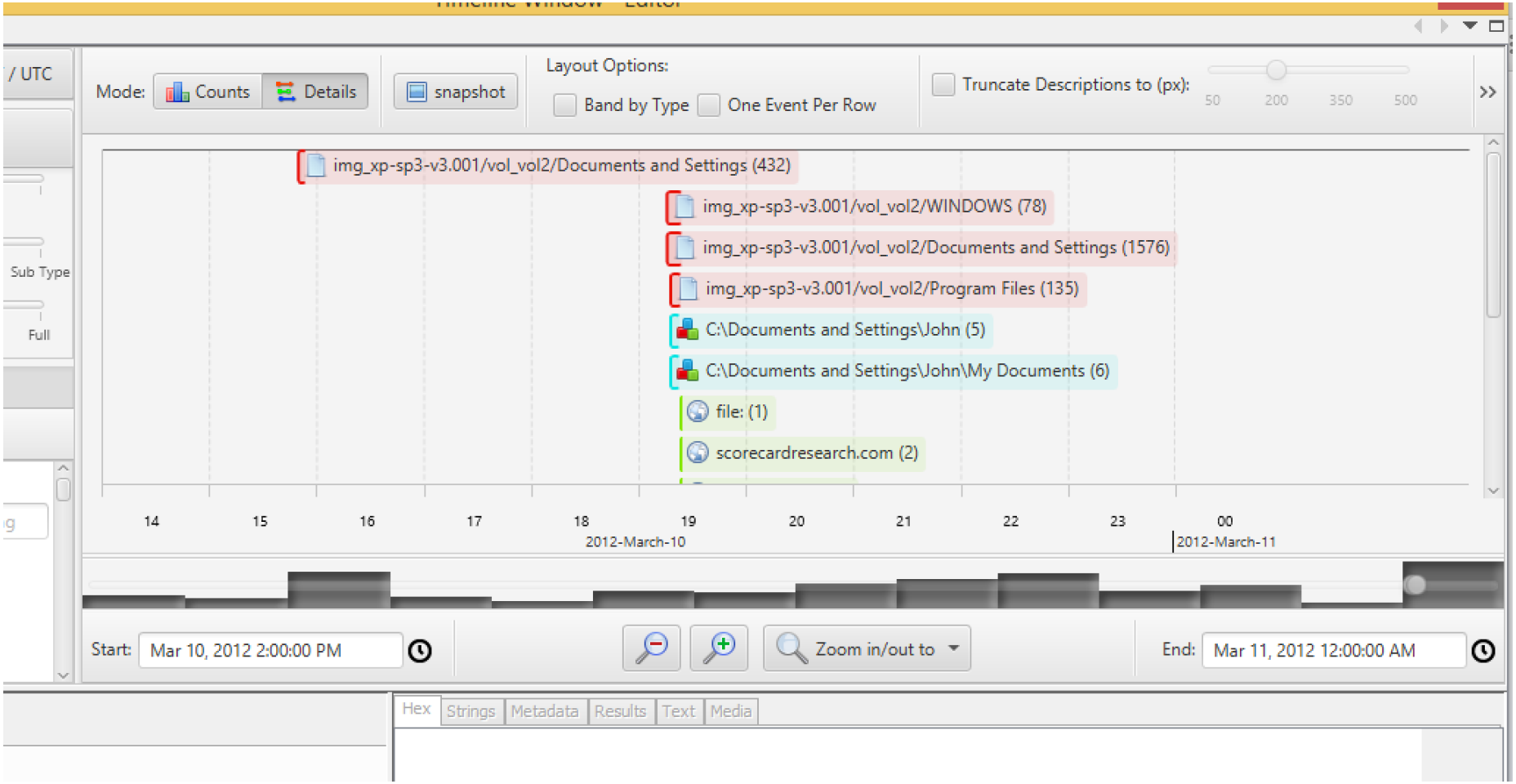
- Build open source and free modules into Autopsy for Law Enforcement use cases.
- Worked with outreach group of local, state, and federal law enforcement.
- Focus areas:
  - Timeline (see Jonathan's talk later today)
  - Image Gallery

New Timeline: How Many Events



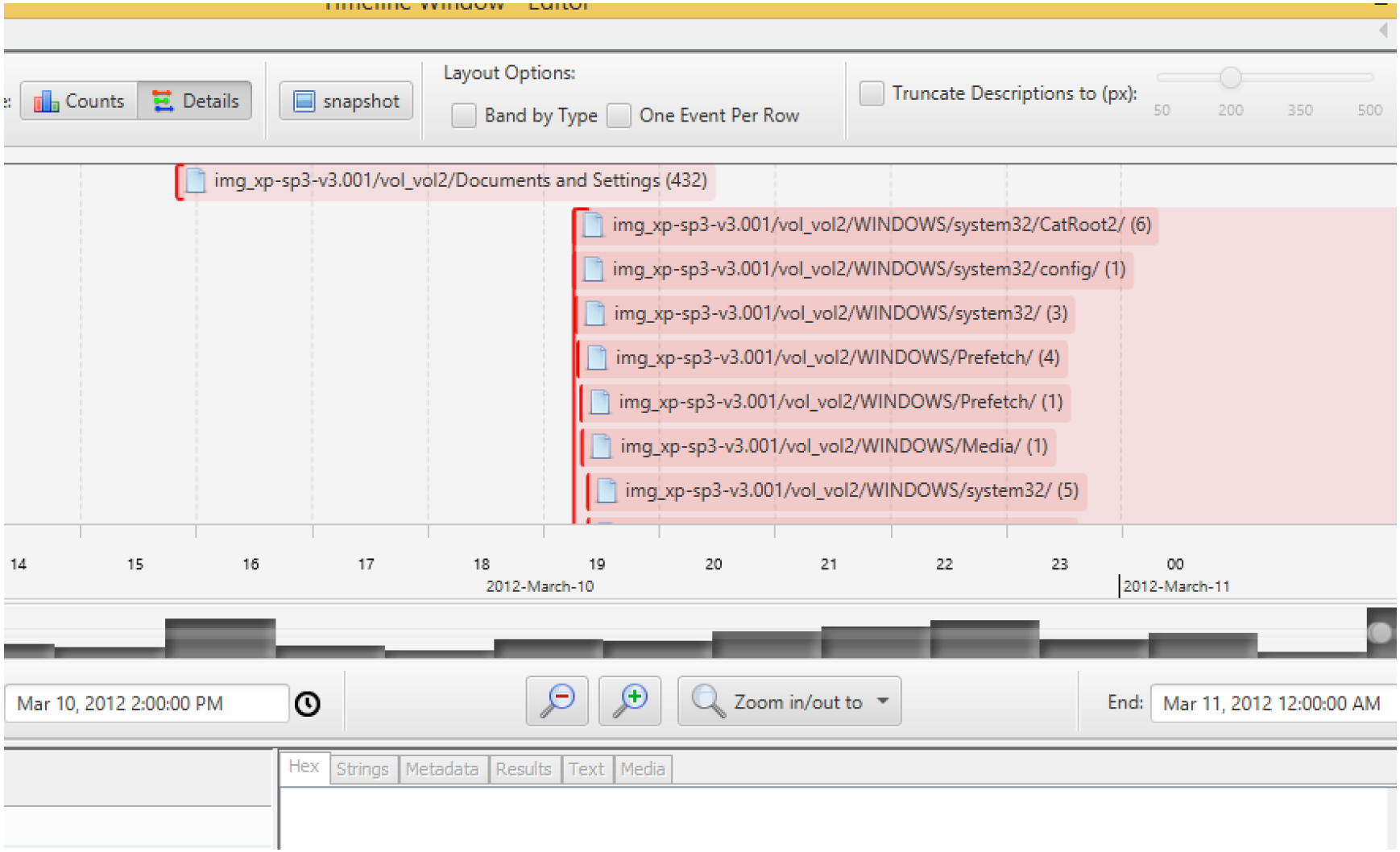
BASIS TECHNOLOGY

New Timeline: What Events



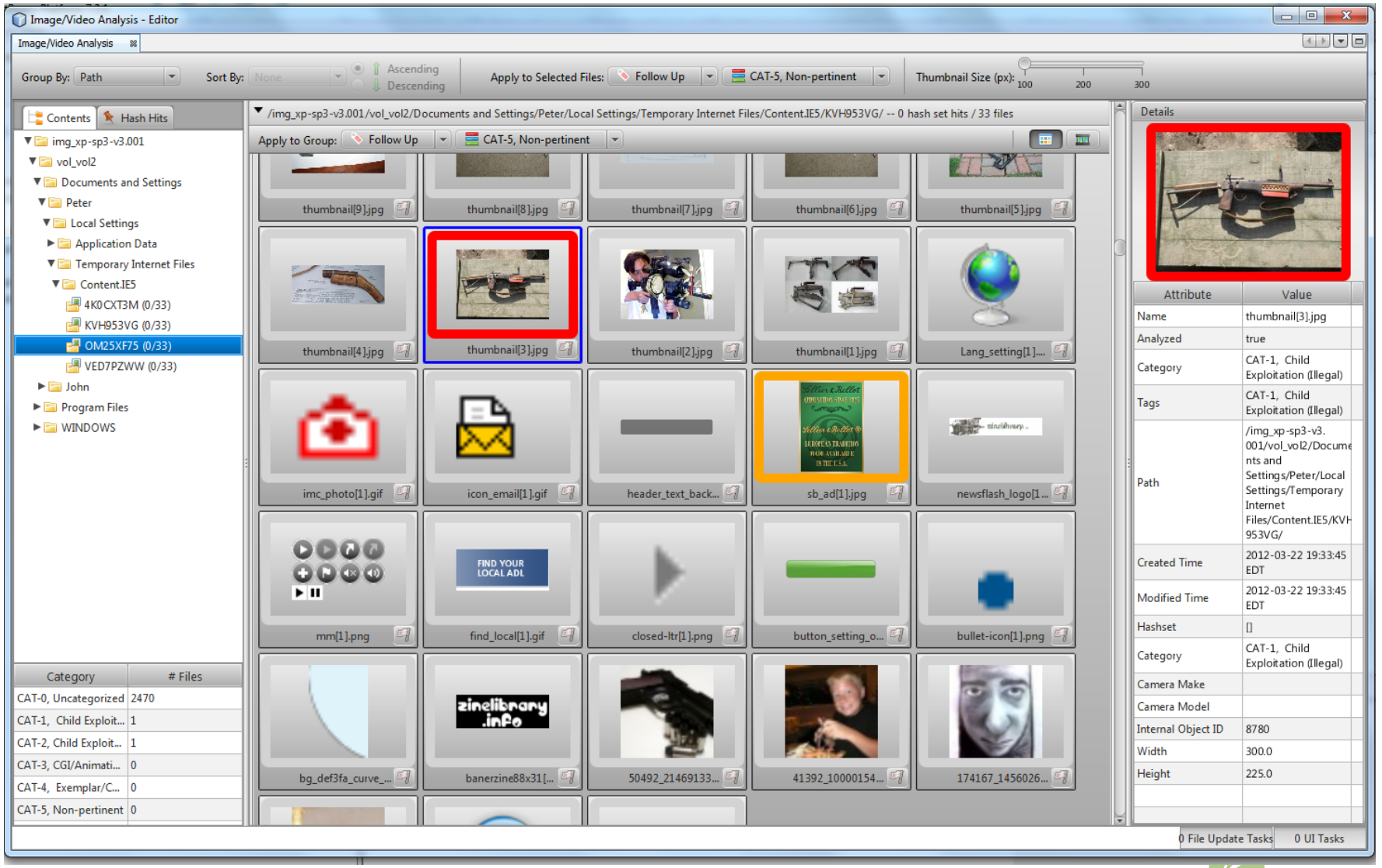
BASIS TECHNOLOGY

Timeline: Zoomed In



BASIS TECHNOLOGY

New Image Gallery (in 3.1.2)



External Modules

- Not Updated to 3.1:
  - Smut Detect: Skin tone (Rajmund Witt)
  - Autopsy AHBM / sdhash (Petter Bjelland)
  - Windows Registry (Willi Ballenthin)
- Updated to 3.1:
  - Multi Content Viewer (Luis Filipe Nassif)
- See: http://wiki.sleuthkit.org/index.php?title=Autopsy_3rd_Party_Modules

Basis: Law Enforcement Bundle

- Integrates Autopsy with child exploitation hash databases.
- Project Vic: ICMEC and US-led effort
- C4All: Canadian-led effort
- Free download from Basis Website.

Basis Module: Cyber Triage

- Incident Response software that automates collection and analysis.
- Remote live collection.
- Automated threat scoring.
- Wizard review process.

Part 3: What's Next

Current Roadmap

- More timeline and image gallery (DHS S&T)
- STIX Module (DHS S&T)
  - See Ann's talk today
- Carving (PhotoRec)
- Keyword Search performance improvements
- More modules TBD

Takeaway

- Has unique features and capabilities.
- If you haven't tried it before, download and try it.

  http://www.sleuthkit.org/autopsy/

- If you have tried it, give us feedback.
- If you have used it in court, let us know.

More Modules Needed

- Community effort is needed.
- Writing Autopsy modules allows you to focus on cool analytics, not:
  - Where is the data coming from
  - How to make a basic UI
  - How to make a basic report
- Reach out to us if you have any questions.

Support

- Community:
  - Sleuthkit-users list
  - Forum.sleuthkit.org
- Commercial:
  - Basis Technology
- Training:
  - 2015 schedule is being determined
  - February online course is open
  - We also do private courses
  - http://www.basistech.com/

Shameless Plug: We're Hiring

- Engineering
  - Full time
  - Interns
- QA and Support

- Contact me (or someone from Basis) for more info.

Name Voting

- Slash
- ROT13 the Rottweiler
- Renzix
- ???

Download Now

http://www.sleuthkit.org/autopsy/