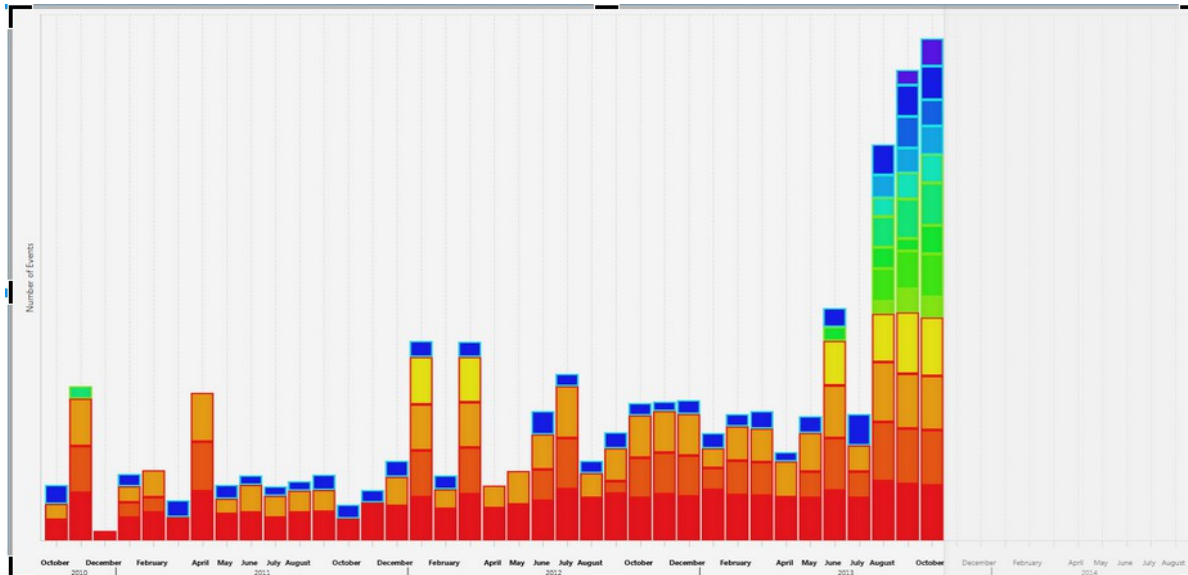
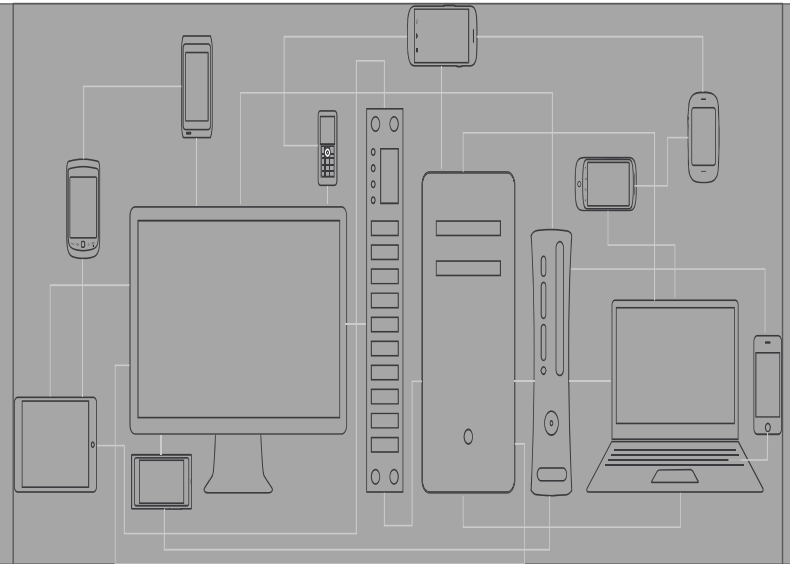


Timeline Visualization in Autopsy

Jonathan Millman



BASIS
TECHNOLOGY

Outline

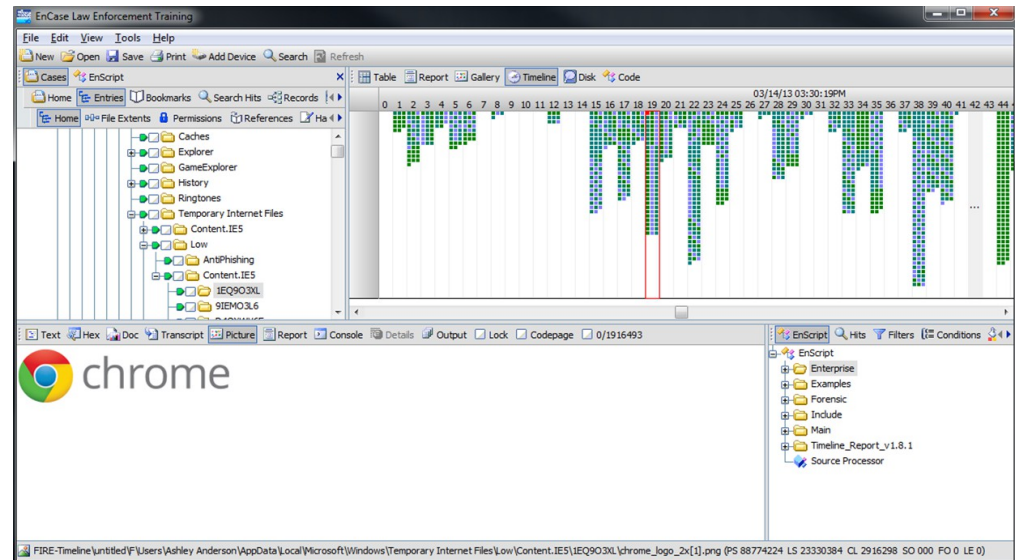
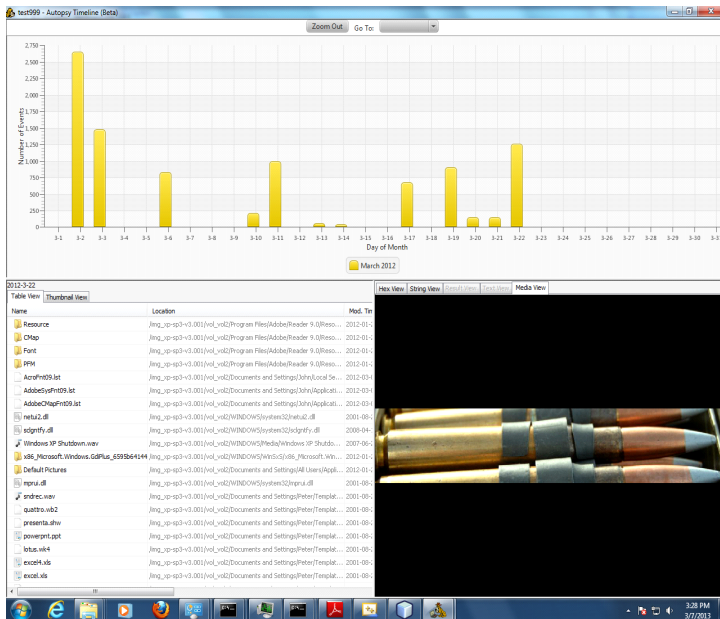
- Project
 - Funding, Motivation , Process, and Design Goals
- Features
 - Data Sources, Zooming, Filtering, Context
- Live Demo

Funding

- Funded by DHS
- Released to open source with Autopsy 3.1.1

Motivation

- Existing timeline analysis tools :
 - don't provide user friendly interfaces
 - don't scale well
 - don't visualize the data in a useful, interactive way



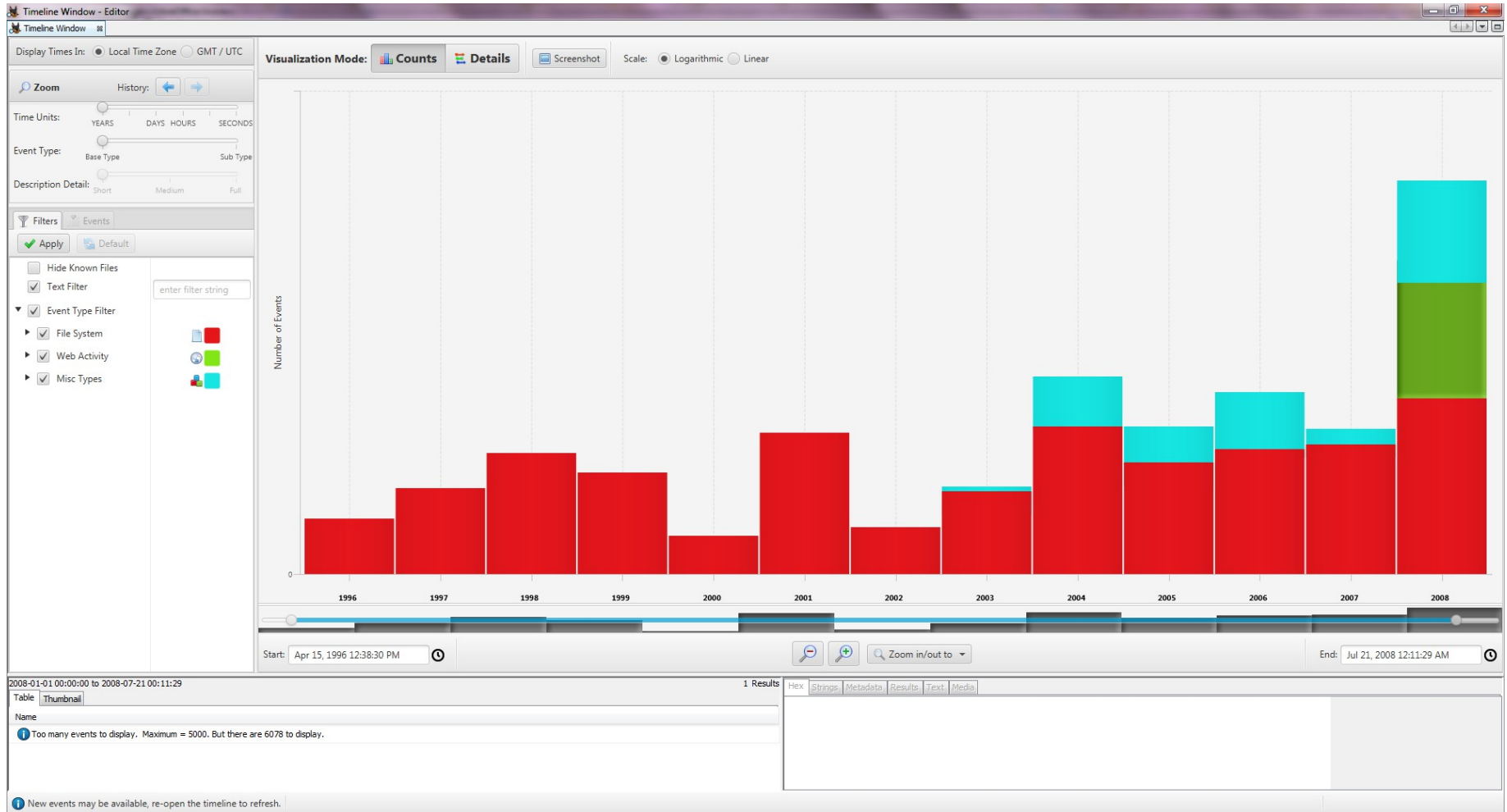
Our Process

- Surveyed 20+ law enforcement officials about what tools they used and their challenges.
- Reviewed non-forensics solutions and techniques.
- Proposed a wireframe to group.
- Built initial beta version.
- Sent beta to group for feedback.
- Built final version.

Design Goals

- Focus first on **visualization** and **usability**
 - Use multiple ways of **zooming** to reduce data to manageable levels
 - Allow **filtering** to further reduce data overload and do targeted searches
 - Provide **context** while exploring the timeline
 - **Scale** to millions of events
- Include **more** than file system events
 - Plaso and other external tools not included yet
- Help answer questions such as:
 - **When** did major web activity occur on a system?
 - **What** websites were accessed that resulted in file system modifications immediately after?

Screen shot



Data Sources

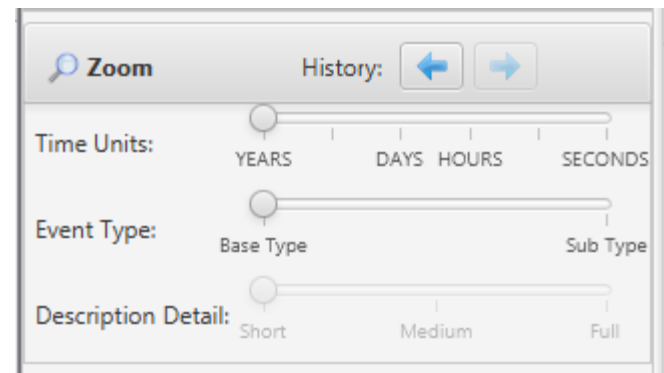
The Timeline feature collects events from *all* Autopsy results with associated timestamps.

Events are stored in a dedicated DB optimized for timelines with millions of events

- File System
 - Modified
 - Access
 - Created
 - Changed
- Web Activity
 - Downloads
 - Cookies
 - Bookmarks (creation)
 - History
 - Searches
- Miscellaneous
 - Email
 - Recent Documents
 - Installed Programs
 - Exif metadata
 - Devices Attached
 - Text Messages (Android)
 - Call Log(Android)
 - GPS Searches(Android)
 - GPS Locations(Android)

Zooming

- Temporal Zooming
 - Entire data set → seconds
 - Multiple ways of adjusting the displayed time range for both precise control and quick and intuitive interaction
- Event Type Zooming
 - Events organized into a taxonomy to support zooming and filtering by the kind of event
- Description Level zooming
 - compose event descriptions at multiple levels of detail
 - Collapse and expand groups of events by different
 - levels of description.



Filtering

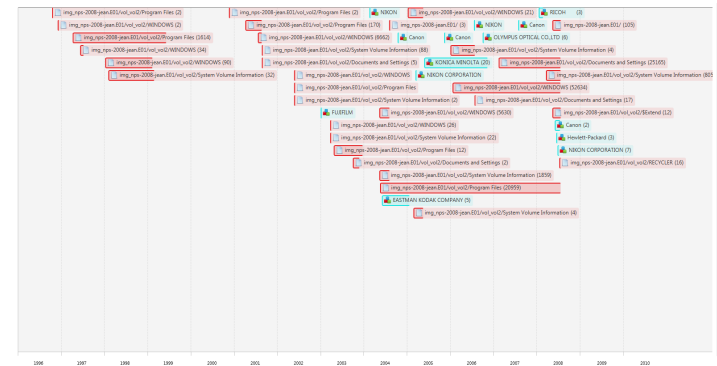
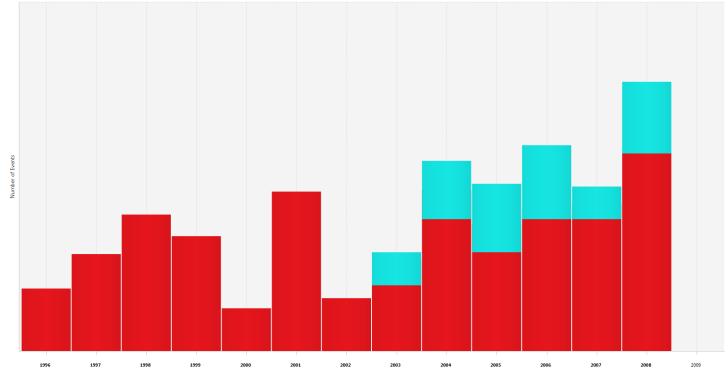
- Reduce data overload and hide uninteresting events
- Temporal zoom functions as kind of filter
- Filter on event type taxonomy
- Substring matching filter on description
- Hide known files (NSRL)

Context

- Understand how it fits into the big picture
- Summary Histogram of entire timeline
- Current Zoom settings overview
- Keep history of zoom and filters to allow quick navigation
- Filter area also doubles as event type color/icon legend
- Visually link events related to selected events

Targeted Visualizations

- When was there activity, and what kind of activity was it?
 - Counts view shows stacked bar chart visualizing the number of events
- What happened at a given time, what else happened before/after?
 - Details view shows exact date/times and details about events.




What now? Actions!

- Use the familiar Autopsy table view and Content Viewer to to examine, export, and tag events

1970-01-13 08:44:31 to 1970-01-13 14:20:21 5 Results

Icon	Date/Time	Description	Base Type	Sub Type	Known
	2004-07-27 13:40:15	EASTMAN KODAK COMPANY : KODAK LS443 ZOOM DIGITAL CAMERA : C2E8E970d01	Misc Types	Exif	UNKNOWN
	2005-01-22 14:10:47	EASTMAN KODAK COMPANY : KODAK LS443 ZOOM DIGITAL CAMERA : 4F571E45d01	Misc Types	Exif	UNKNOWN
	2004-06-03 10:03:59	EASTMAN KODAK COMPANY : KODAK LS443 ZOOM DIGITAL CAMERA : 42961214d01	Misc Types	Exif	UNKNOWN
	2004-11-06 11:51:54	EASTMAN KODAK COMPANY : KODAK LS443 ZOOM DIGITAL CAMERA : BEF5AC2E.d01	Misc Types	Exif	UNKNOWN
	2004-08-09 17:57:46	EASTMAN KODAK COMPANY : KODAK LS443 ZOOM DIGITAL CAMERA : 57761251d01	Misc Types	Exif	UNKNOWN

Hex Strings Metadata Results [next](#) Media



in reports!

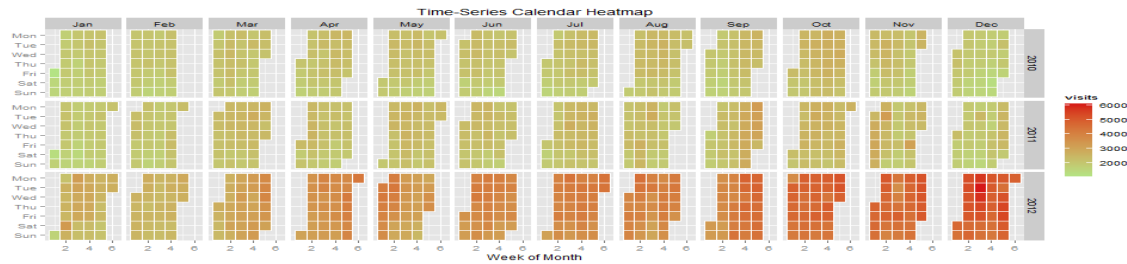
◦ Live Demo !!

- backup video <http://basistech.wistia.com/medias/dotnhpo882>

Going Forward

- Some improvements we are thinking about
 - More data sources:** plaso / log2timeline
 - dynamic description level grouping** based on time range and number of events
 - Cyclical / Calendar Visualization** to help spot patterns of activity

better layout



Inspiration from <http://www.tatvic.com/blog/calender-heatmap-with-google-analytics-data/>

Questions

