

7<sup>th</sup> Annual

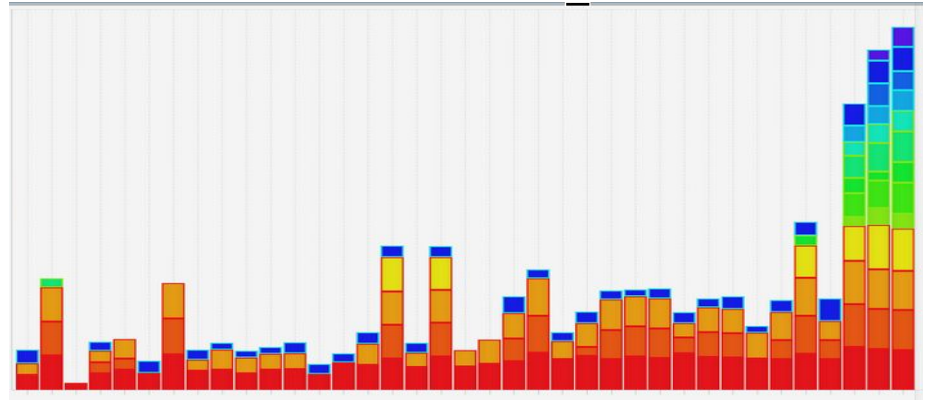
# #OSDFCon

OPEN SOURCE DIGITAL FORENSICS CONFERENCE



## Timeline Visualization in Autopsy

Jonathan Millman



- Funded by DHS S&T
- Released to open source with Autopsy 3.1.1
- Significant enhancements by 4.2

# Outline

1. High Level Overview
2. Example Scenarios
3. Live Demo
4. Questions

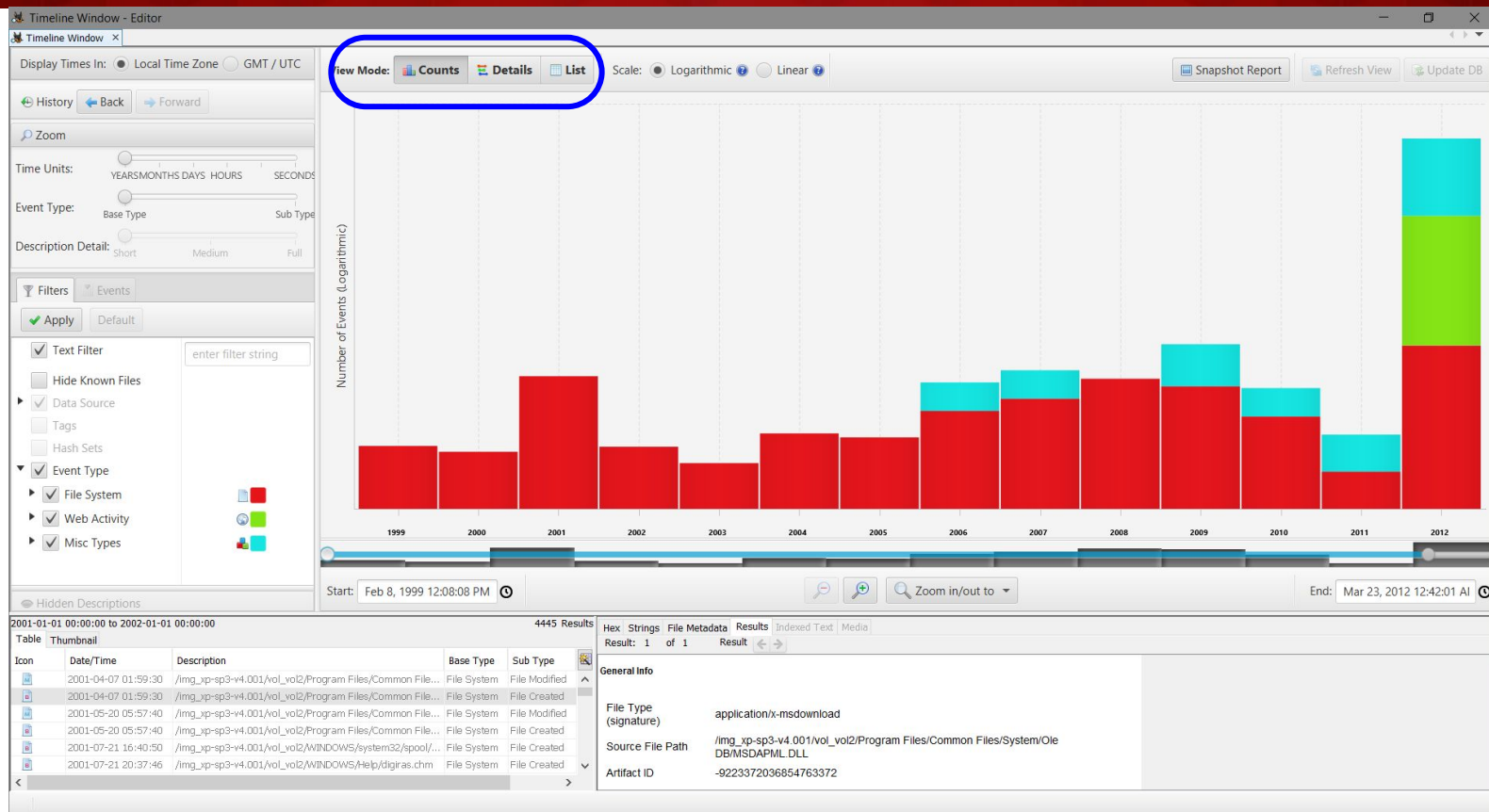
# Overview

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

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

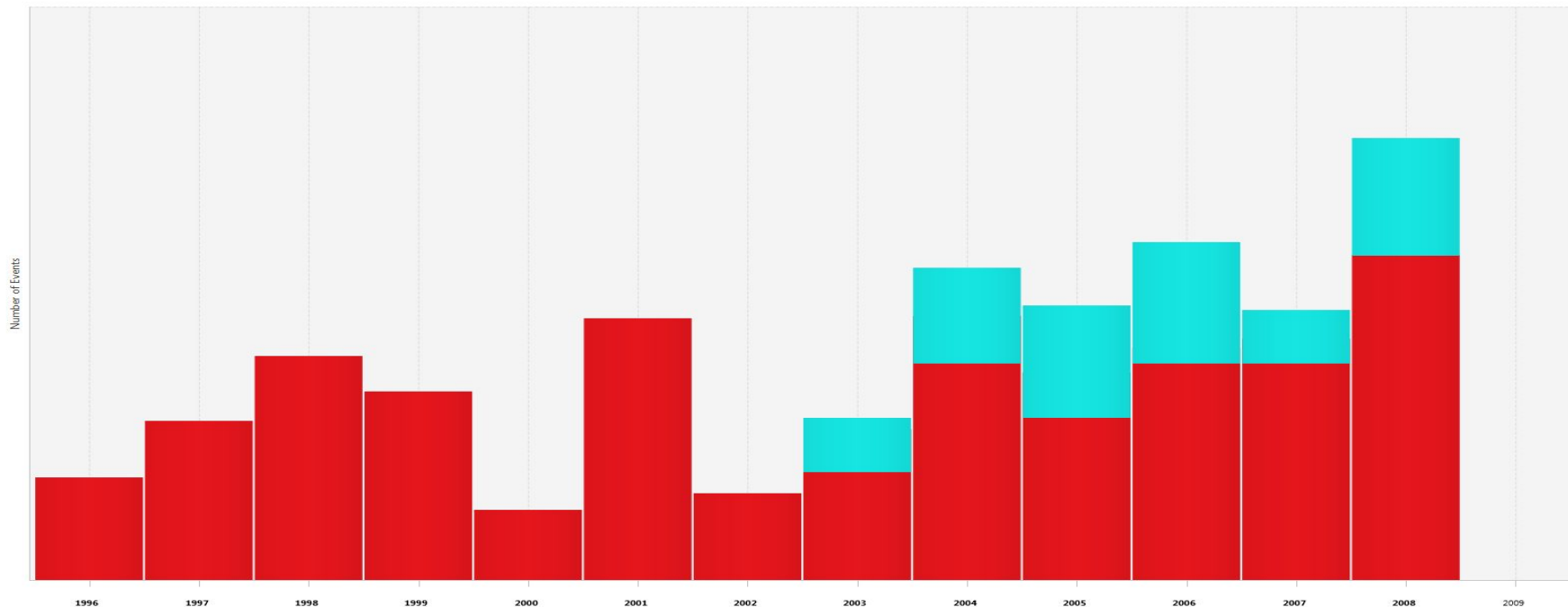
- File System
  - Modified
  - Access
  - Created
  - Changed
- Web Activity
  - Downloads
  - Cookies
  - Bookmarks (creation)
  - History
  - Searches
- Miscellaneous
  - Email
  - Recent Documents
  - Installed Programs
  - Exif metadata
  - Devices Attached
  - Text Messages (Android)
  - Call Log(Android)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

# Overview



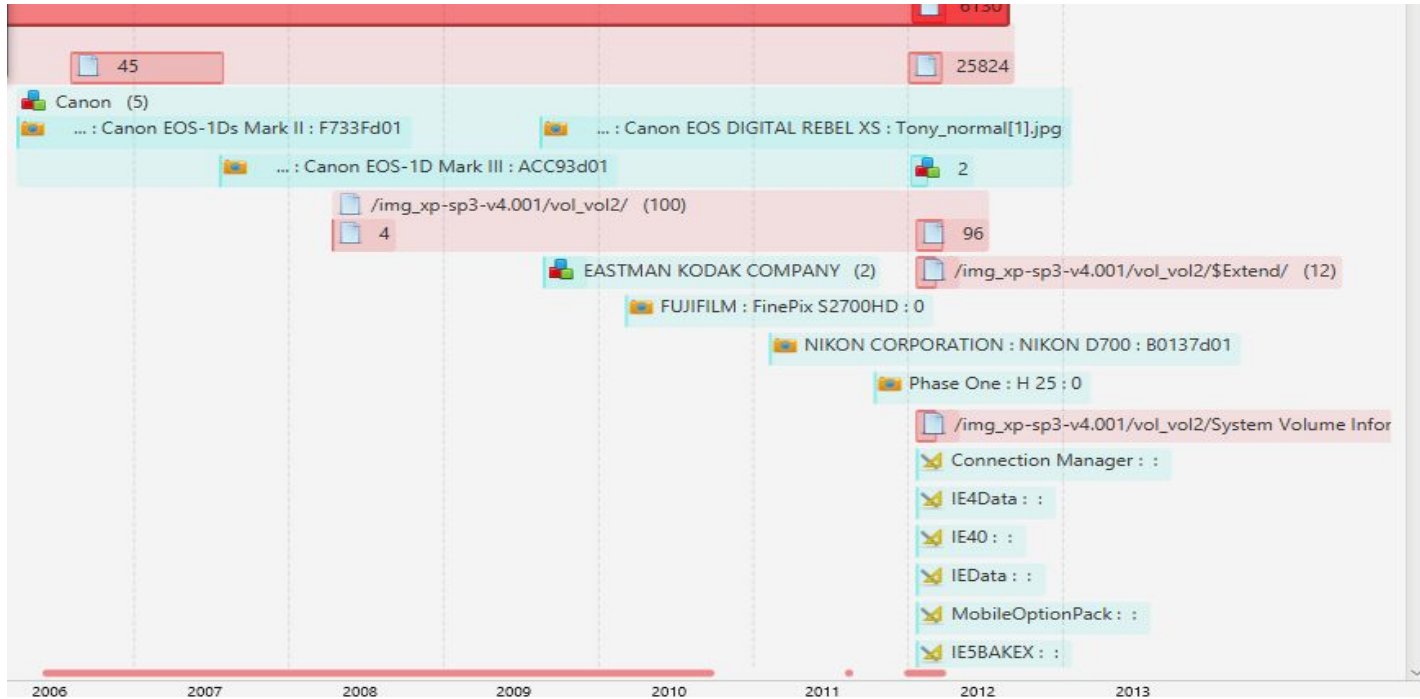
# Overview: Counts View

When was there activity, and what kind of activity was it?



# Overview: Details View


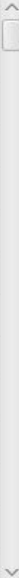













What happened at a given time, what else happened before/after?





# Overview: List View

I just want to see the details of every event in chronological order!

37,005 events				
Date/Time	Event Type	Description	Known	+
1999-02-08 12:08:08	 M__B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Comm ... d/web server extensions/40/bin/1033/FPEXT.MSG	known	
1999-04-14 21:46:54	 M__B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Resource/Font/PFM/SY____.PFM	known	
1999-04-14 21:46:54	 M__B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Resource/Font/PFM/zx____.pfm	known	
1999-04-14 21:46:54	 M__B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Resource/Font/PFM/zy____.pfm	known	
1999-04-14 21:46:54	 M__B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Resource/Font/SY____.PFB	known	
1999-04-14 21:46:54	 M__B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Resource/Font/ZX____.PFB	known	
1999-04-14 21:46:54	 M__B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Resource/Font/ZY____.PFB	known	
1999-06-06 10:09:26	 M__B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Com ... les/Microsoft Shared/Web Folders/MSOWS409.DLL	known	
2000-07-24 23:47:08	 M__B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/vdk150.dll	known	
2000-09-28 02:49:58	 M__B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/Optional/README.TXT	known	
2000-10-09 20:44:50	 M__B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Resource/CMap/Identity-H	known	
2000-10-09 20:44:50	 M__B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Resource/CMap/Identity-V	known	
2000-11-19 17:28:36	 M__B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Comm ... ared/web server extensions/40/bin/FP4AWEC.DLL	known	
2001-04-07 01:59:30	 M__B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Common Files/System/Ole DB/MSDAPML.DLL	known	

Zooming:

Showing more or less details,  
sometimes at the cost of excluding  
some data (temporal zooming)

Filtering:

Reduce data overload with composable filters. Do more targeted searches.

Context:

Maintain awareness of how the current view fits into the larger case.

# Example Scenarios

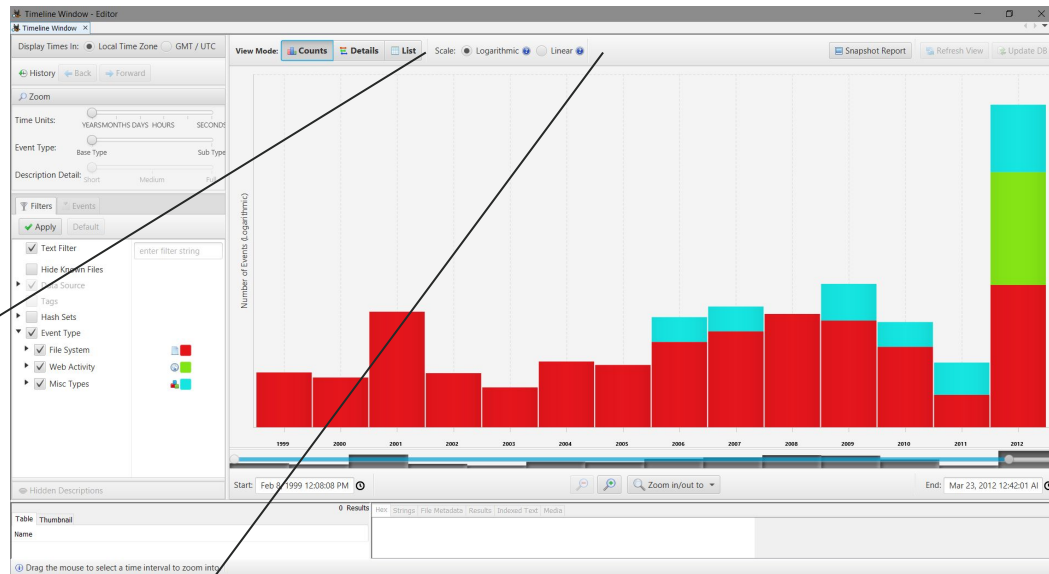
# Scenario 1

You have a new computer:  
You want to find out what was  
happening in the last days.

# Scenario 1: Counts View

Shows number and type of events.

Interaction is with bars in chart

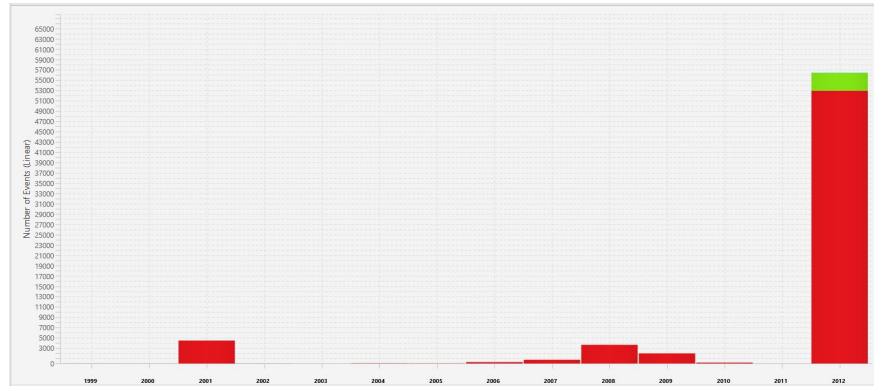


Scale: ☐ Logarithmic ☒ Linear

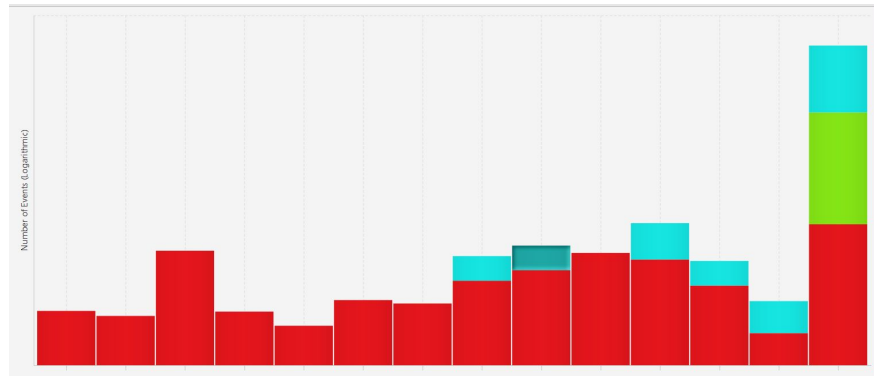
Two scale options

# Scenario 1: Counts View

Linear Scale shows directly proportional counts

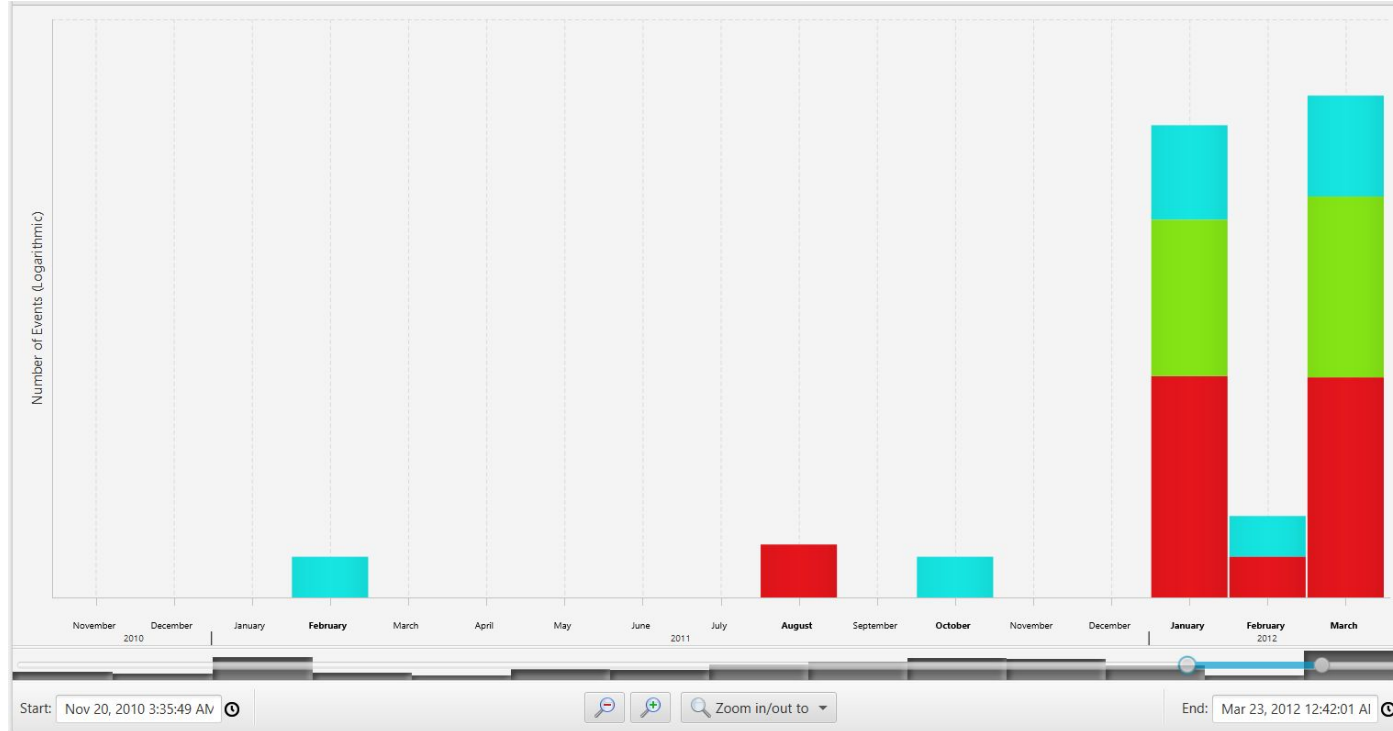


Logarithmic Scale compresses the range of counts, and makes relatively small counts visible. Can be hard to interpret, use with caution.



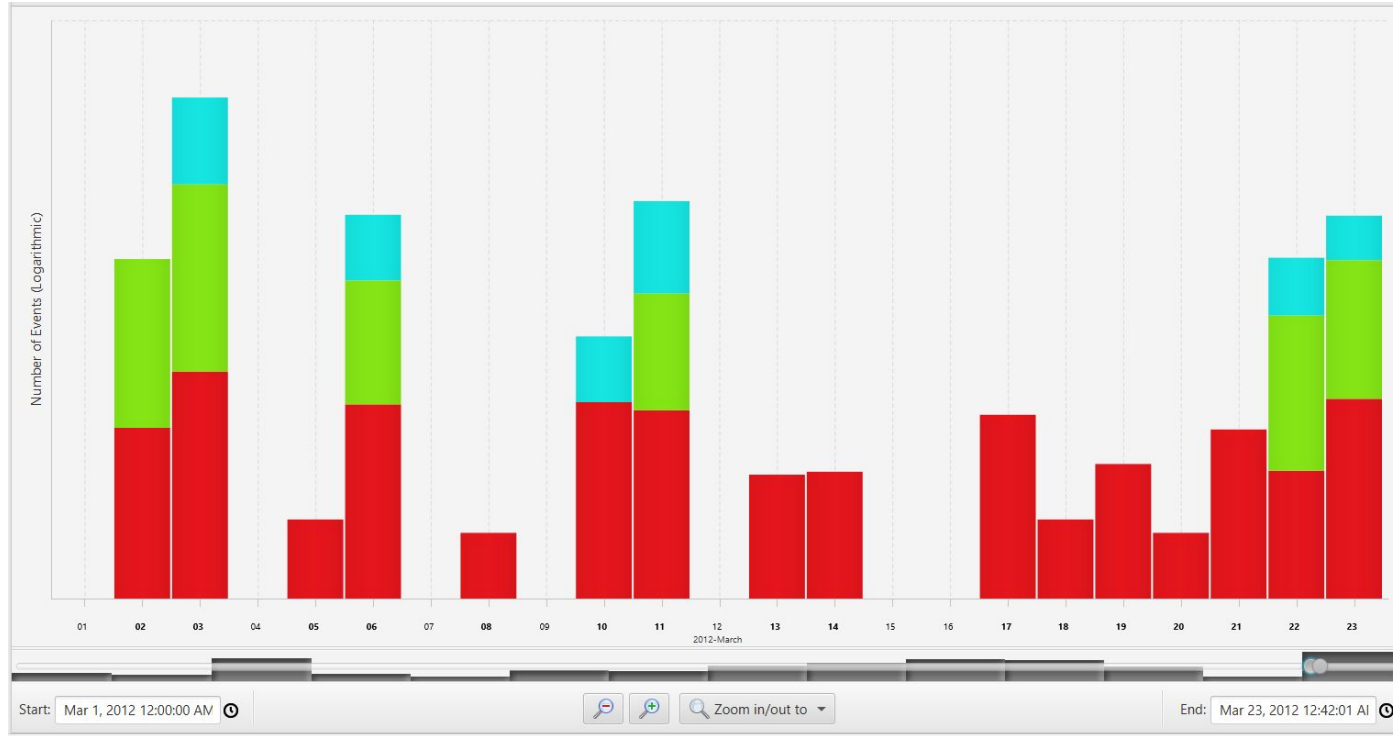


# Scenario 1: Counts View



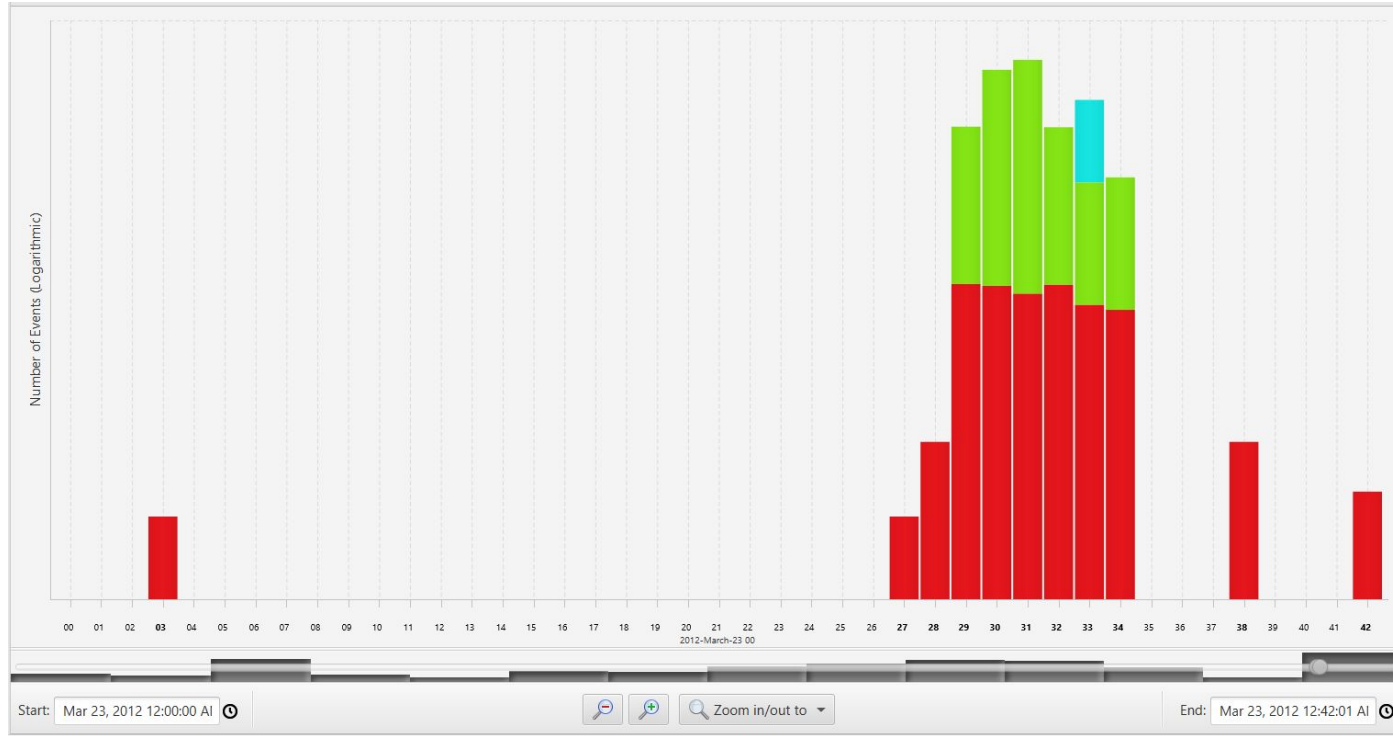
Drag the range slider to zoom in.

# Scenario 1: Counts View



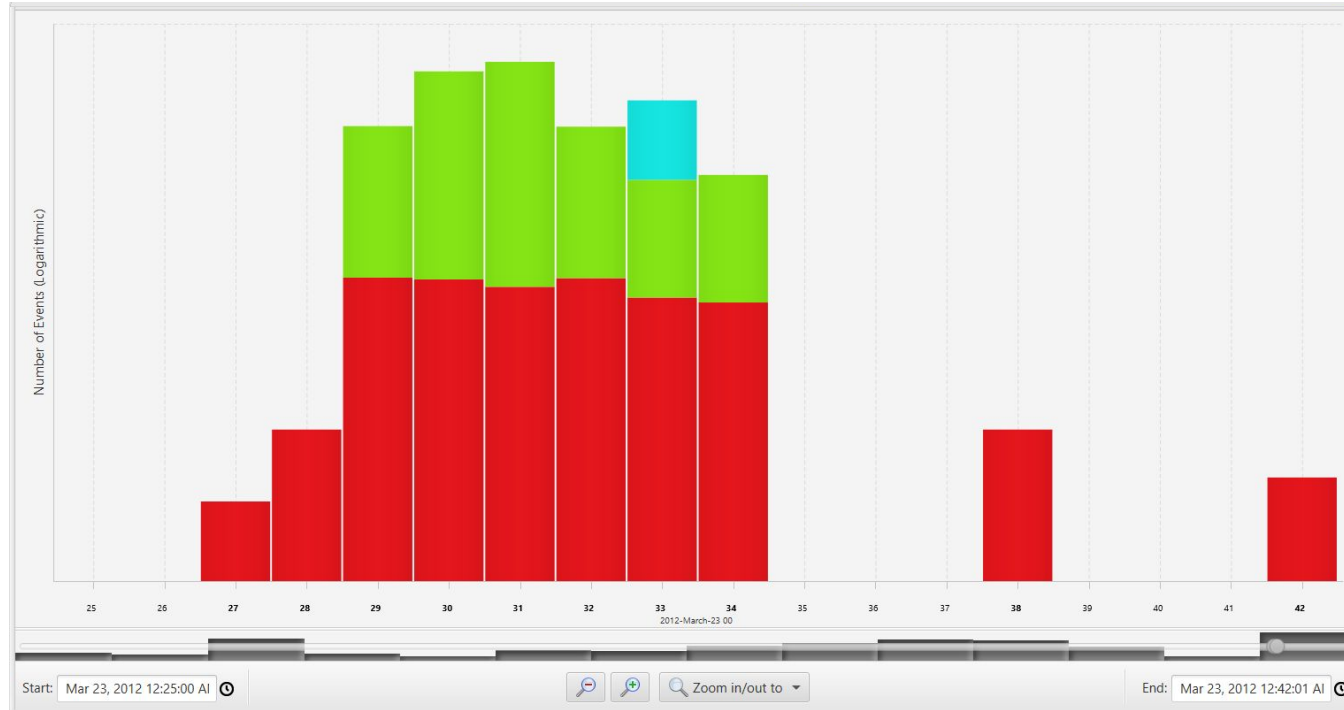
Double click last month to zoom in.

# Scenario 1: Counts View



Double click last day to zoom in again.

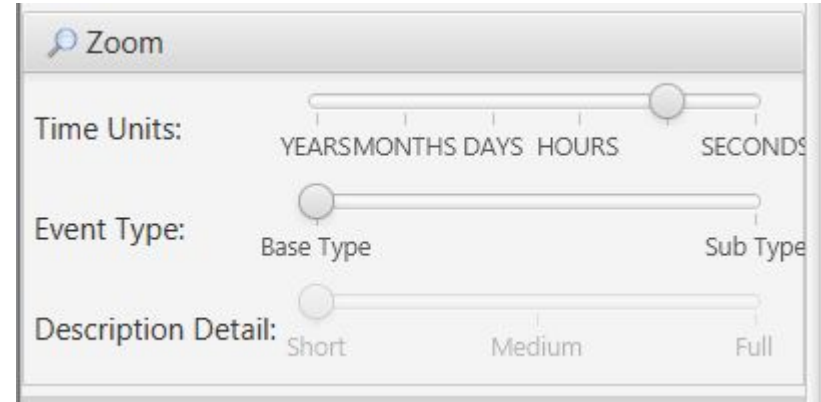
# Scenario 1: Counts View



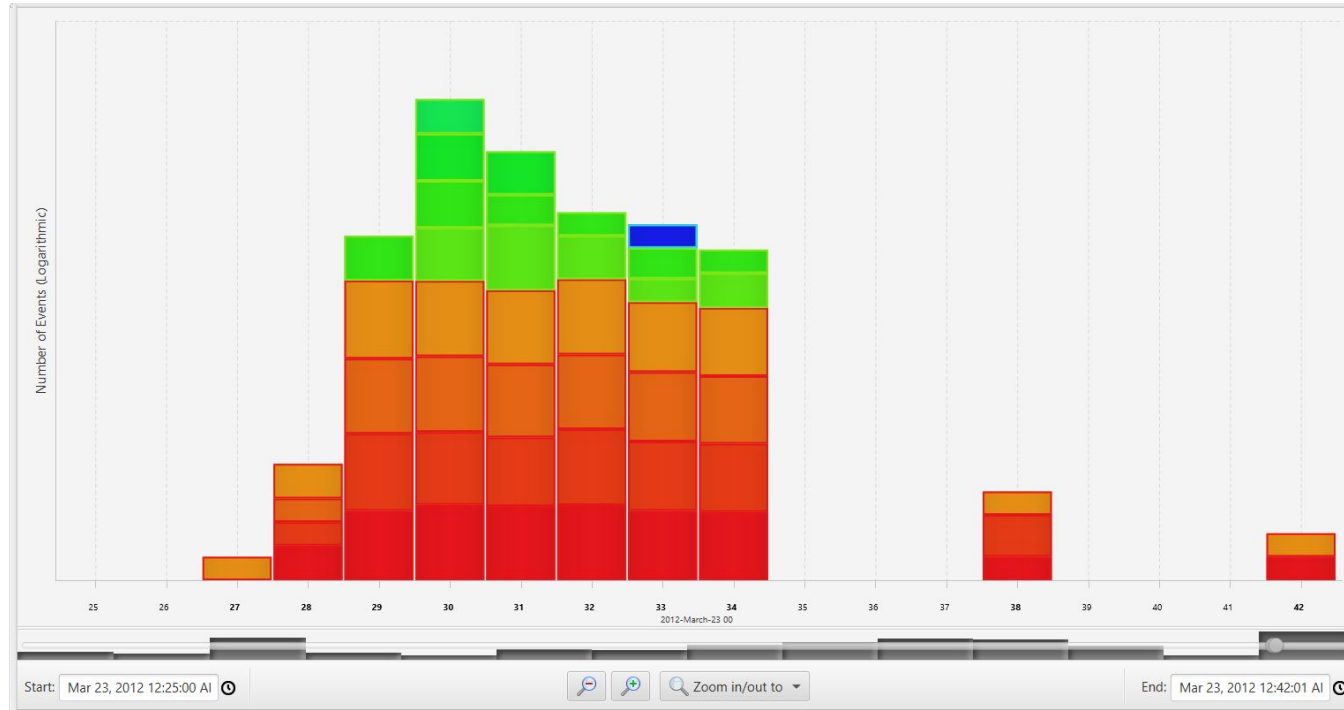
Drag out a selector to zoom to arbitrary time range

# Scenario 1: Zooming

Multiple other ways of zooming in time for both precise control and quick intuitive interaction



# Scenario 1: Counts View

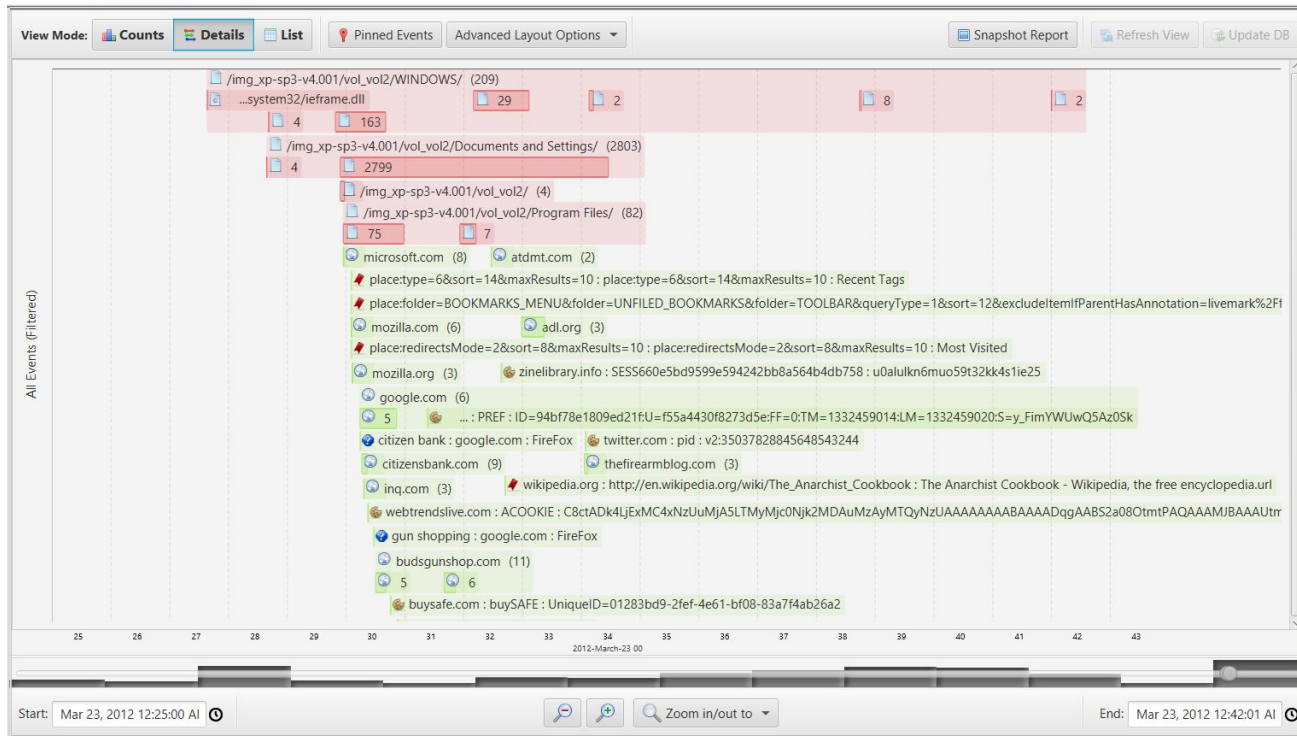


Break out event sub types.

# Scenario 1

You've gotten a feel for when there was activity on the system. But what was it exactly?

# Scenario 1: Details View










Switch to details view



# Scenario 1: Details View

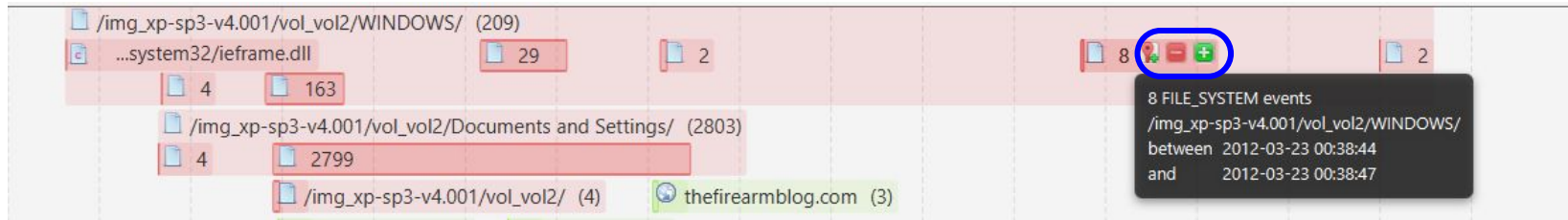
Details View clusters events by time, type, and description. Allows free form exploration of events.

## User Actions

Expand and collapse descriptions	 
Hide/show events by description	 
Pin events to maintain context	 
Place guide marker	

# Scenario 1: Details View

What are those outliers?

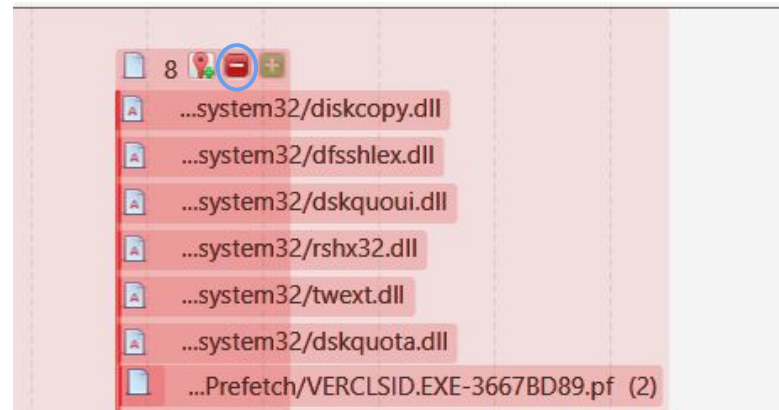
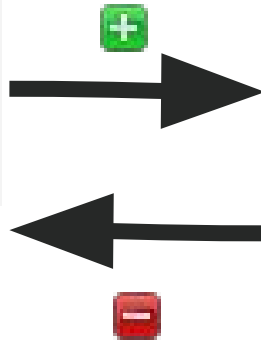


Expand groups based on description to find out

# Scenario 1: Details View



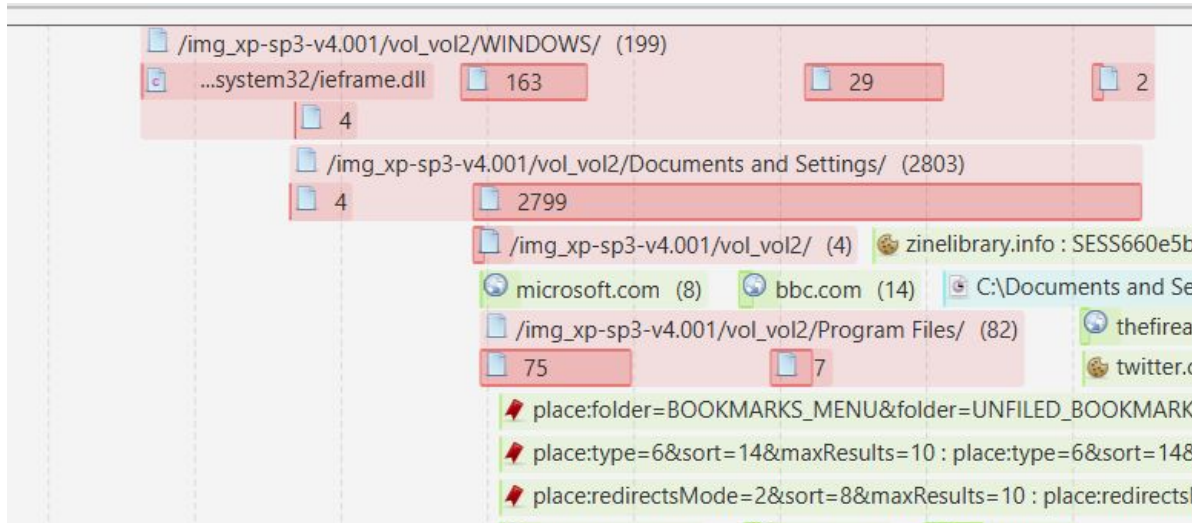
Expand /collapse cluster to next level of description



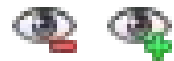
They don't look too interesting. You could adjust the time range to exclude them.

# Scenario 1: Details View

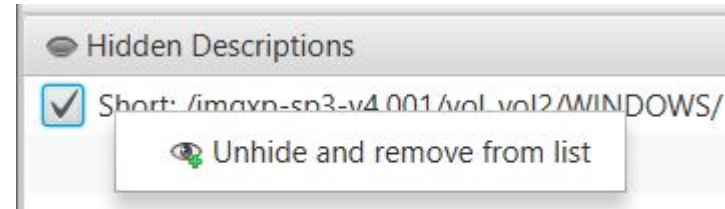
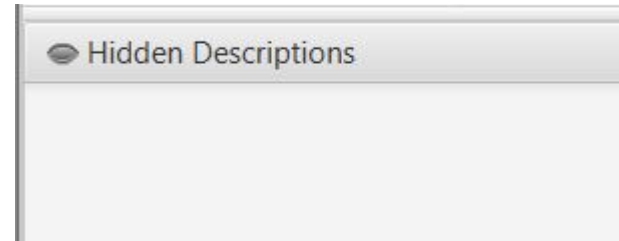
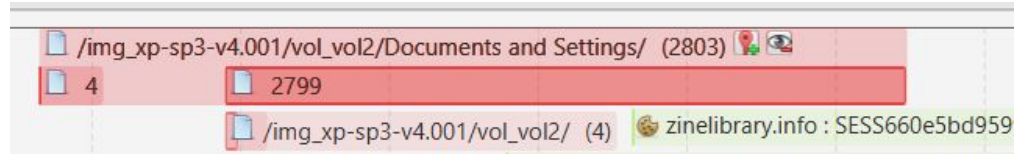
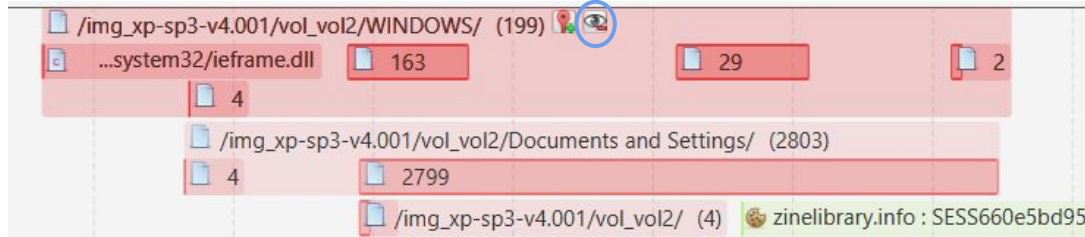
Let's say that no files in the WINDOWS folder are interesting. Lets hide them.



# Scenario 1: Details View



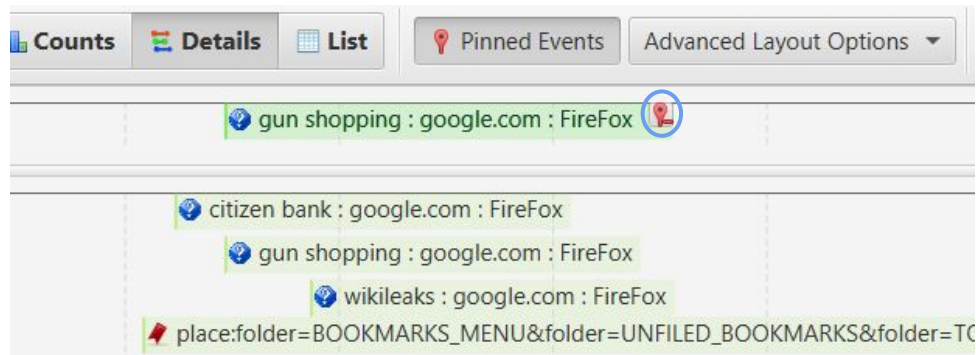
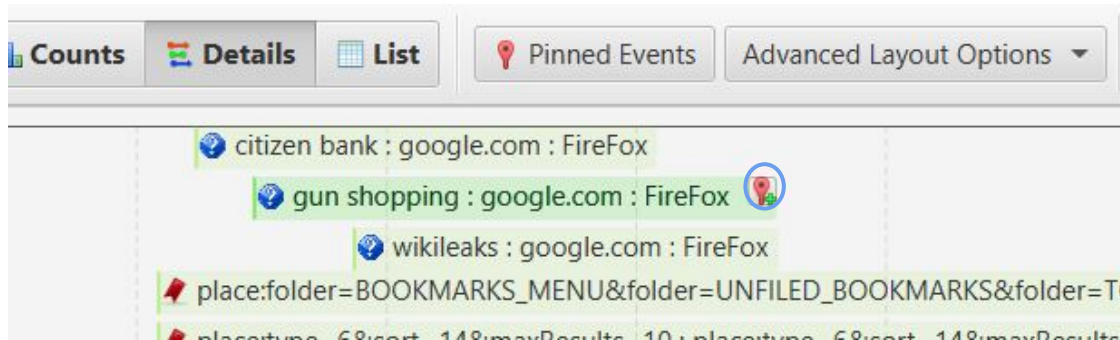
Hide and show event clusters by description



# Scenario 1: Details View



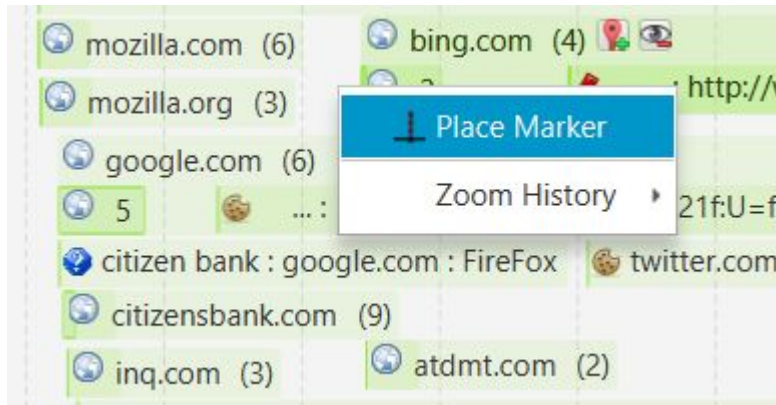
Pin events to maintain context



# Scenario 1: Details View

┃ Place guide markers as references you explore

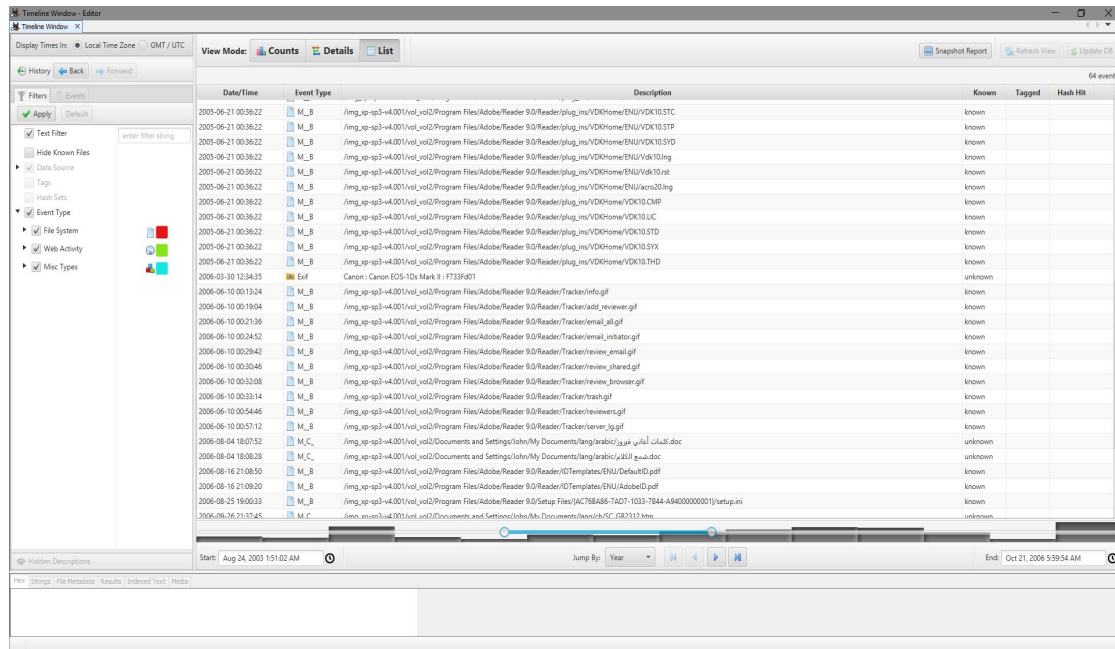
The guide marker is useful for quickly assessing the relative times of events in the visualization. For permanent marking, use pinning.



You have run ingest with a hash list: You want to find out what was happening around hash hits.



# Scenario 2: List View



By popular demand!

Switch after exploring  
in Counts/Details

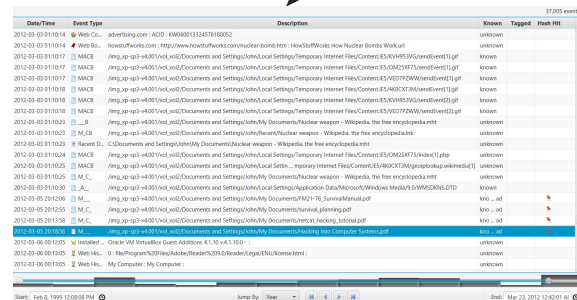
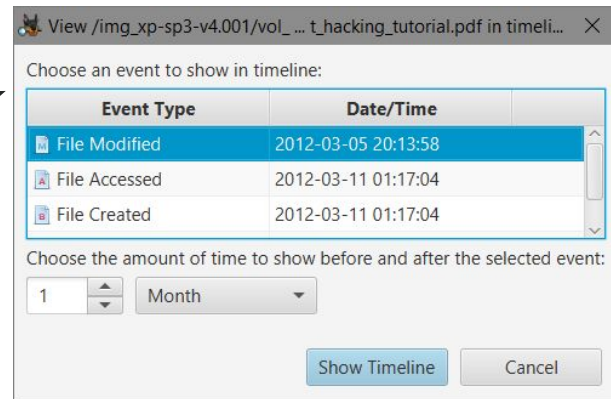
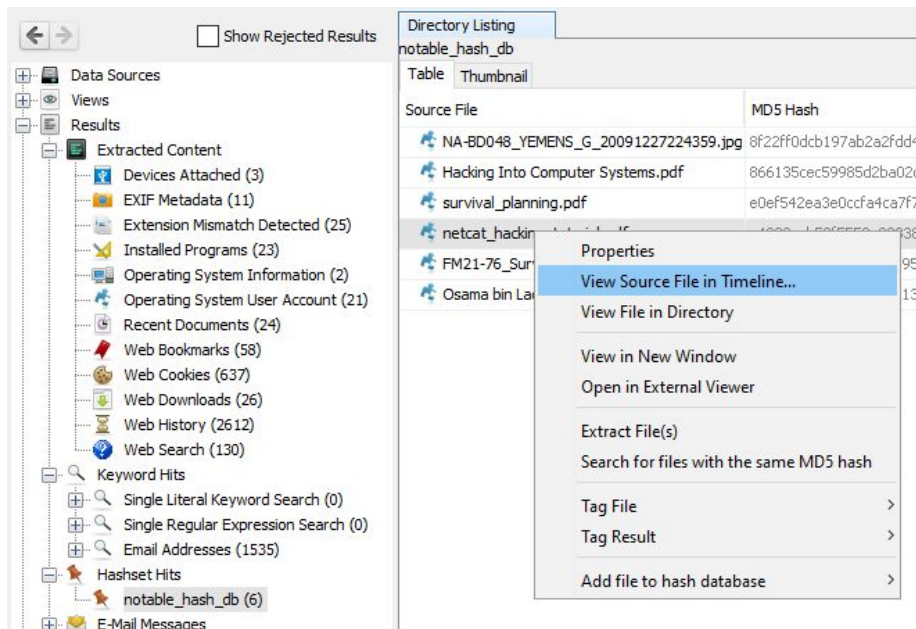
Or

Jump directly to  
listview from Autopsy

Zooming no longer makes sense, but time selection still works as a filter.

# Scenario 2: List View

## Jumping directly to List View from Autopsy



# Scenario 2: List View

Adding a text filter, reduces the view to 20 events

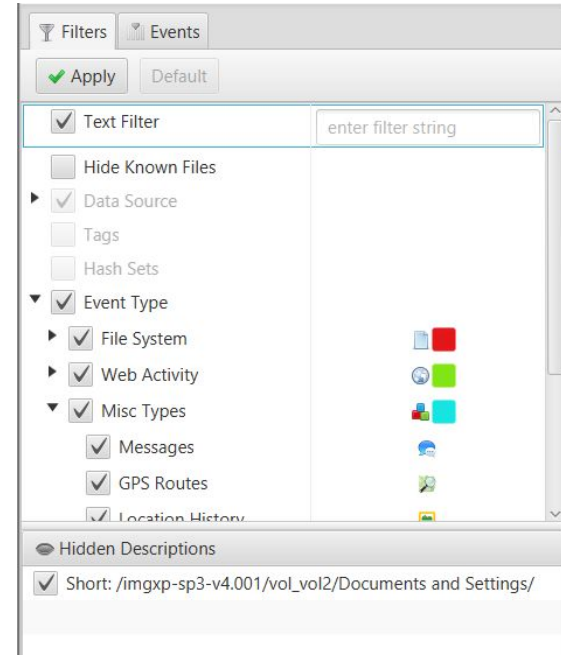
20 events

Date/Time	Event Type	Description	Known	Tagged	Hash Hit	+
2012-03-03 01:02:27	Web His...	google.com : http://www.google.com/#hl=en&client=psy-ab&q=hackin ... =ebada0e4be87c9aa&biw=800&bih=509 : hacking guide - Google Search	unknown			
2012-03-03 01:02:27	Web Sea...	hacking guide : google.com : Chrome	unknown			
2012-03-03 01:02:30	Web His...	google.com : http://www.google.com/url?sa=t&rct=j&q=hacking%20gu ... q9rT8qGJKTX0QHs6jJBg&usg=AFQjCNFICbYFIOcRZYq4FVp56EuG9CSDKg :	unknown			
2012-03-03 01:02:30	Web Sea...	hacking guide : google.com : Chrome	unknown			
2012-03-03 01:02:32	Web His...	google.com : http://www.google.com/url?sa=t&rct=j&q=hacking%20gu ... q9rT8qGJKTX0QHs6jJBg&usg=AFQjCNHArEwAFXISJ2oiv_O7moFq5pm5ig :	unknown			
2012-03-03 01:02:32	Web Sea...	hacking guide : google.com : Chrome	unknown			
2012-03-03 01:02:34	Web Co...	puremango.co.uk : __utmz : 156180964.1330732954.1.1.utmcsrc=google[utmccn=(organic)]utmcmd=organic[utmctr=hacking%20guide	unknown			
2012-03-03 01:02:34	Web His...	puremango.co.uk : http://www.puremango.co.uk/2004/12/how_to_hack_79/ : How To Hack – Beginners Guide to Hacking Computers	unknown			
2012-03-03 01:02:43	Web Bo...	puremango.co.uk : http://www.puremango.co.uk/2004/12/how_to_hack_79/ : How To Hack – Beginners Guide to Hacking Computers	unknown			
2012-03-05 20:13:58	M_C_	/img_xp-sp3-v4.001/vol_vol2/Documents and Settings/John/My Documents/netcat_hacking_tutorial.pdf	kno ... ad			
2012-03-05 20:18:56	M_...	/img_xp-sp3-v4.001/vol_vol2/Documents and Settings/John/My Documents/Hacking Into Computer Systems.pdf	kno ... ad			
2012-03-10 20:45:58	_A_	/img_xp-sp3-v4.001/vol_vol2/Documents and Settings/John/Recent/Hacking Into Computer Systems.Ink	unknown			
2012-03-11 00:22:14	Web His...	file : file/Documents%20and%20Settings/John/My%20Documents/Hacking%20Into%20Computer%20Systems.pdf :	unknown			
2012-03-11 00:22:14	Web His...	file : file/Documents%20and%20Settings/John/My%20Documents/Hacking%20Into%20Computer%20Systems.pdf :	unknown			
2012-03-11 01:17:04	_B	/img_xp-sp3-v4.001/vol_vol2/Documents and Settings/John/My Documents/Hacking Into Computer Systems.pdf	kno ... ad			
2012-03-11 01:17:04	_A_B	/img_xp-sp3-v4.001/vol_vol2/Documents and Settings/John/My Documents/netcat_hacking_tutorial.pdf	kno ... ad			
2012-03-11 01:22:14	_C_	/img_xp-sp3-v4.001/vol_vol2/Documents and Settings/John/My Documents/Hacking Into Computer Systems.pdf	kno ... ad			
2012-03-11 01:22:14	M_CB	/img_xp-sp3-v4.001/vol_vol2/Documents and Settings/John/Recent/Hacking Into Computer Systems.Ink	unknown			
2012-03-11 01:22:14	Recent D...	C:\Documents and Settings\John\My Documents\Hacking Into Computer Systems.pdf	unknown			
2012-03-19 19:07:36	_A_	/img_xp-sp3-v4.001/vol_vol2/Documents and Settings/John/My Documents/Hacking Into Computer Systems.pdf	kno ... ad			

# Scenario 2: Filtering

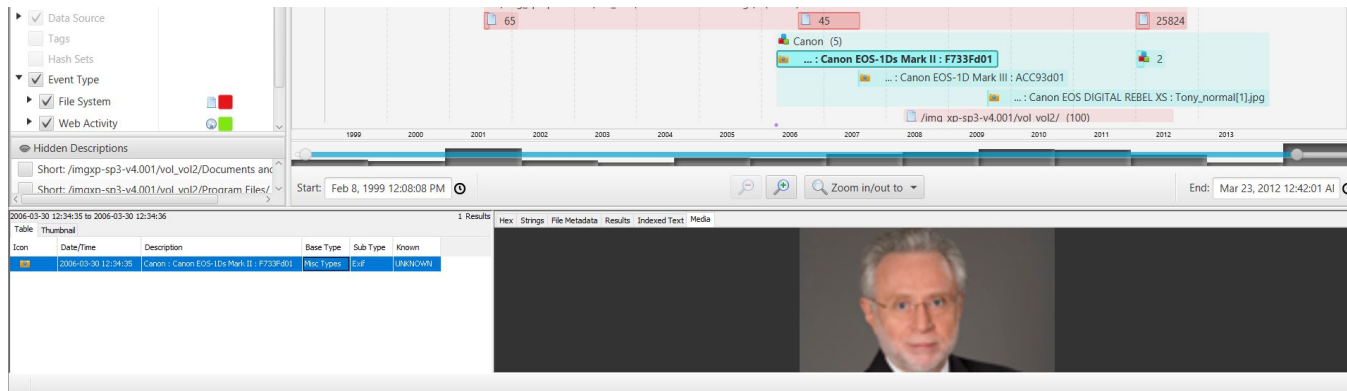
Reduce data overload and hide uninteresting events

Filter on:  
Description, known  
status, event type, data  
sources, tags, hash  
sets

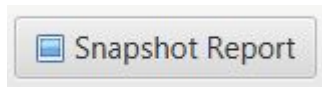


# What now?

Use the familiar Autopsy table/thumbnail views and content viewers to examine, tag, and export events.



Take a screen-shot of the visualization for inclusion in reports!



# Going Forward

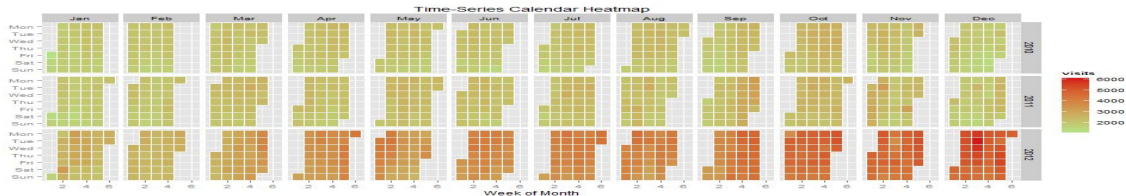
Some improvements we are thinking about

## **Integrate with Collaborative Autopsy**

**More data sources:** plaso / log2timeline , custom / manual events

**Dynamic description level grouping** based on time range and number of events

**Cyclical / Calendar visualization** to help spot patterns of activity



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

# Live Demo !!



# Questions

