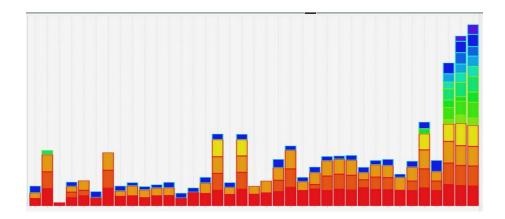
Tth Annual **CONTRACT STATE**



OPEN SOURCE DIGITAL FORENSICS CONFERENCE

Timeline Visualization in Autopsy

Jonathan Millman



October 26, 2016 | Westin Washington Dulles, Herndon, VA

Brief Intro



- 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

Overview



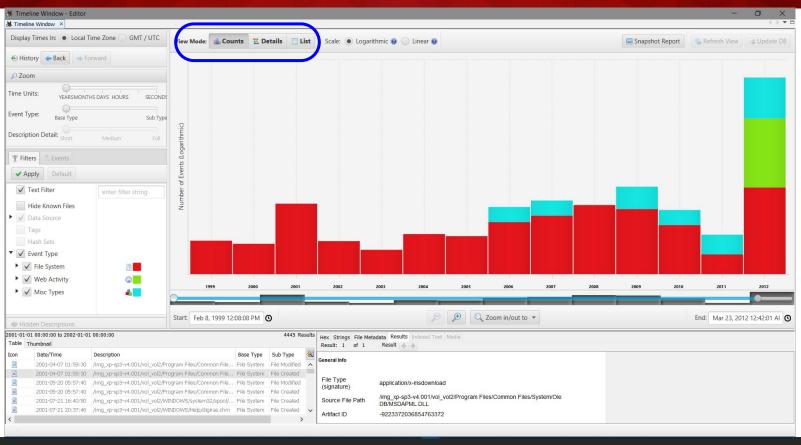
The Timeline feature includes events from *all* Autopsy results with associated timestamps.

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

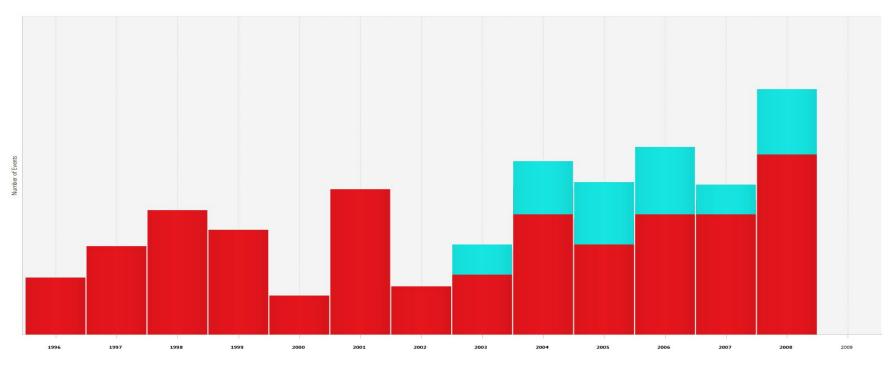




Overview: Counts View



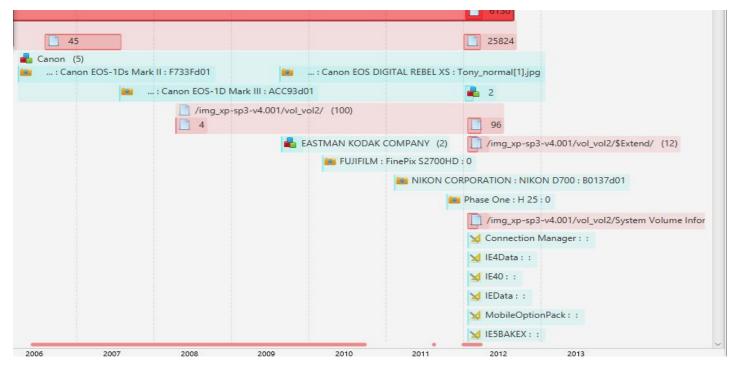
When was there activity, and what kind of activity was it?



Overview: Details View



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





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

			37,005 ev	ent
Date/Time	Event Type	Description	Known	
1999-02-08 12:08:08	MB	/img_xp-sp3-v4.001/vol_vol2/Program Files/Comm d/web server extensions/40/bin/1033/FPEXT.MSG	known	ŕ
1999- <mark>04-14 21:46:5</mark> 4	MB	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Resource/Font/PFM/SYPFM	known	1
1999-04-14 21:46:54	MB	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Resource/Font/PFM/zxpfm	known	
1999-04-14 2 <mark>1:46:5</mark> 4	MB	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Resource/Font/PFM/zypfm	known	
1999-04-14 21:46:54	MB	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Resource/Font/SYPFB	known	
1999- <mark>04-14 21:46:5</mark> 4	MB	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Resource/Font/ZXPFB	known	
1999-04-14 21:46:54	MB	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Resource/Font/ZYPFB	known	
1999-06-06 10:09:26	MB	/img_xp-sp3-v4.001/vol_vol2/Program Files/Com les/Microsoft Shared/Web Folders/MSOWS409.DLL	known	
2000-07-24 23:47:08	MB	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/vdk150.dll	known	
2000-09-28 02:49:58	MB	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/Optional/README.TXT	known	
2000-10- <mark>0</mark> 9 20:44:50	MB	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Resource/CMap/Identity-H	known	
2000-10 <mark>-</mark> 09 20:44:50	MB	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Resource/CMap/Identity-V	known	
2000-11-19 17:28:36	MB	/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	

Overview: Common Themes



Zooming:

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

Overview: Common Themes



Filtering:

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

Overview: Common Themes



Context:

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



Example Scenarios



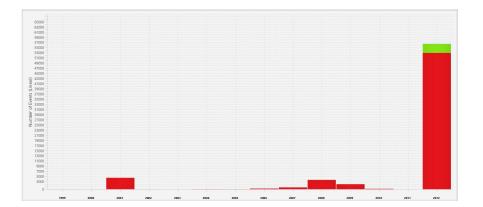
You have a new computer: You want to find out what was happening in the last days.



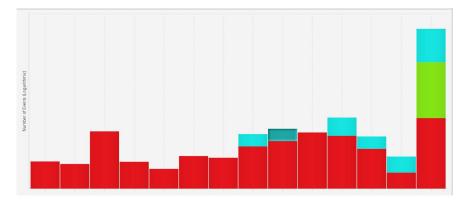




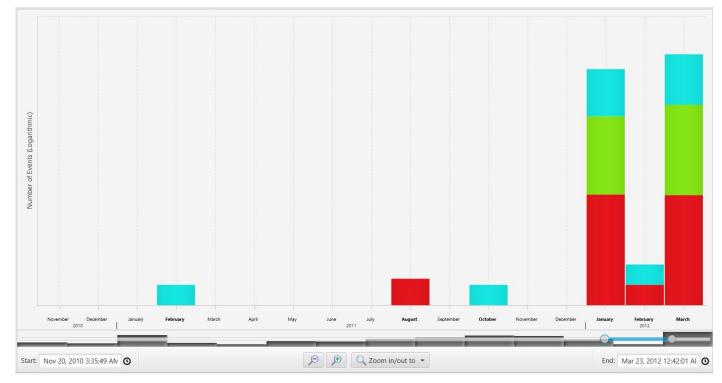
Linear Scale shows directly proportional counts



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

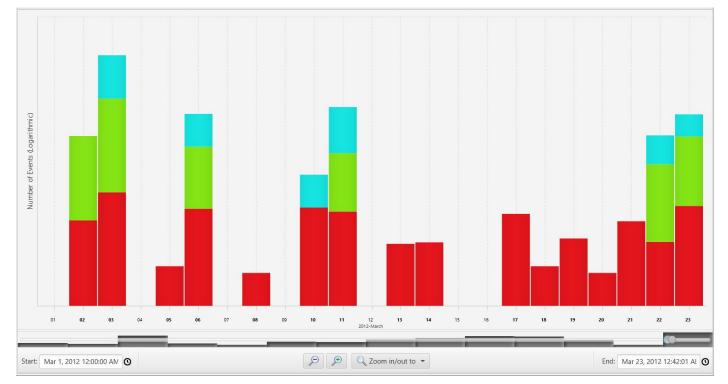






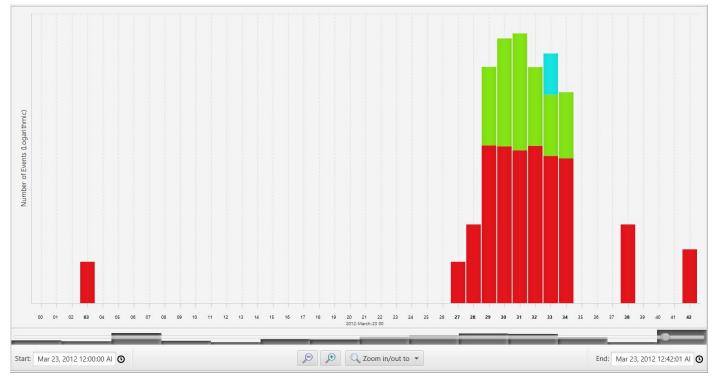
Drag the range slider to zoom in.





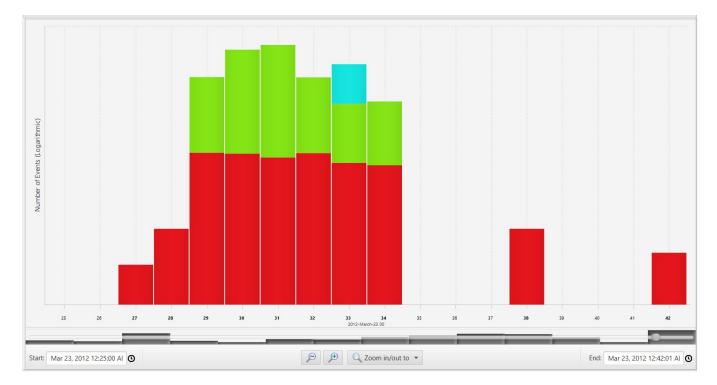
Double click last month to zoom in.





Double click last day to zoom in again.





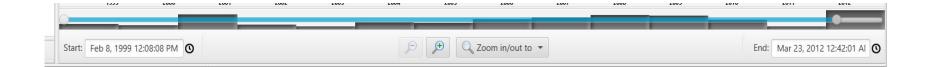
Drag out a selector to zoom to arbitrary time range

Scenario 1: Zooming

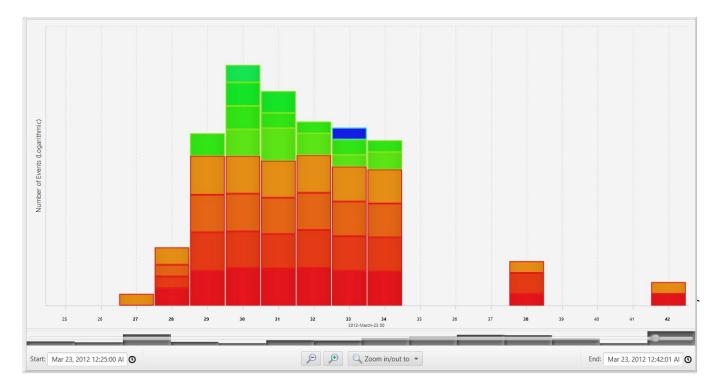


Multiple other ways of zooming in time for both precise control and quick intuitive interaction

D Zoom			0
Time Units:	YEARSMONTHS	DAYS HOURS	
Event Type:	Base Type		Sub Type
	etail: Short	Medium	Full







Break out event sub types.



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



	/img xp-sp3-	/4.001/vol_vol2/WINDOWS/ (209)
	system32,	
	4	163
	☐ /im ☐ 4	g_xp-sp3-v4.001/vol_vol2/Documents and Settings/ (2803) 2799 img_xp-sp3-v4.001/vol_vol2/ (4)
		//mg_xp-sp3-v4.001/v0L_v0L2/Program Files/ (82)
		microsoft.com (8) atdmt.com (2)
		place:type=6&sort=14&maxResults=10:place:type=6&sort=14&maxResults=10:Recent Tags
		place:folder=BOOKMARKS_MENU&folder=UNFILED_BOOKMARKS&folder=TOOLBAR&queryType=1&sort=12&excludeItemIfParentHasAnnotation=livemark%2
		S mozilla.com (6) adl.org (3)
		Comozilla.org (3) since zina zina zina zina zina zina zina zina
		google.com (6) google.com (6) s weight = 10 = 94bf78e1809ed21ftU=f55a4430f8273d5e:FF=0:TM=1332459014:LM=1332459020:S=v FimYWUwQ5Az0Sk
		(c) (c)
		Citizensbank.com (9)
		G inq.com (3) 🕴 wikipedia.org : http://en.wikipedia.org/wiki/The_Anarchist_Cookbook : The Anarchist Cookbook - Wikipedia, the free encyclopedia.url
		webtrendslive.com : ACOOKIE : C8ctADk4LjExMC4xNzUuMjA5LTMyMjc0Njk2MDAuMzAyMTQyNzUAAAAAAABAAAAQqAABS2a08OtmtPAQAAAMJBAAAUt
		gun shopping : google.com : FireFox
		budsgunshop.com (11) 5 6
		🍪 buysafe.com : buySAFE : UniqueID=01283bd9-2fef-4e61-bf08-83a7f4ab26a2
25 26	27 28	29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 2012-March-23 00

Switch to details view



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

User Actions

Expand and collapse descriptions	E
Hide/show events by description	@ @
Pin events to maintain context	% %
Place guide marker	1



What are those outliers?

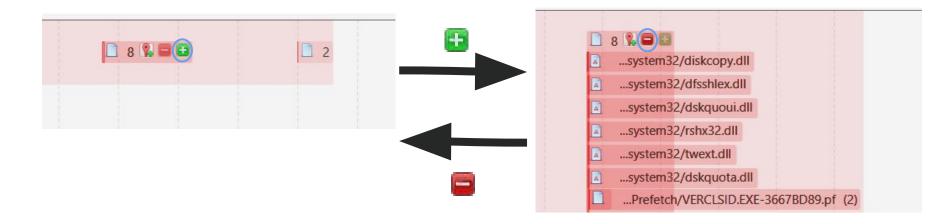


Expand groups based on description to find out





Expand /collapse cluster to next level of description



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



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

	/img_xp-sp3-v4.001/vol_v	ol2/WINDOWS/ (199)		
0	system32/ieframe.dll	163	29	2
	4			
	/img_xp-sp	3-v4.001/vol_vol2/Docume	nts and Settings/ (28	03)
	4	2799		
		/img_xp-sp3-v4.001/	/vol_vol2/ (4) 🚳 zin	elibrary.info : SESS660e5b
		S microsoft.com (8)	S bbc.com (14)	C:\Documents and Se
		/img_xp-sp3-v4.001	/vol_vol2/Program Fil	es/ (82) 😡 thefirea
		75	7	🎯 twitter.
		🕴 place:folder=BOO	KMARKS_MENU&fold	er=UNFILED_BOOKMAR
		🕴 place:type=6&sor	t=14&maxResults=10	: place:type=6&sort=148
		Place:redirectsMod	de=2&sort=8&maxRe	esults=10 : place:redirects

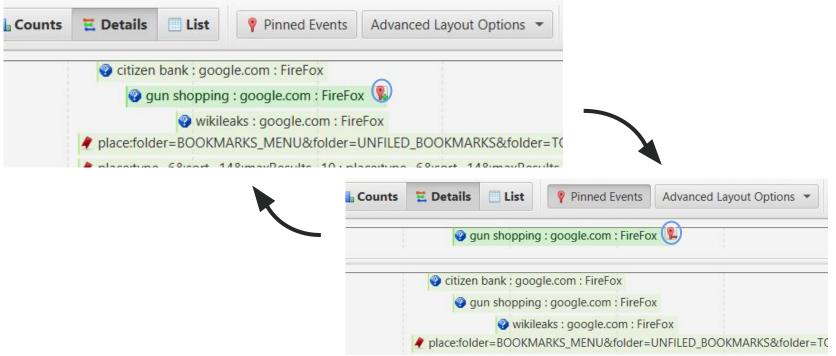


Hide and show event clusters by description

/img_xp-sp3-v4.001/vol_v system32/ieframe.dll	vol2/WINDOWS/ (199) 🕵 😨	29	2	Hidden Descriptions	
/img_xp-sj	p3-v4.001/vol_vol2/Documents a 2799 (img_xp-sp3-v4.001/vol_v		nfo : SESS660e5bd95		
	₩				
/img_xp-sp3-v4.(001/vol_vol2/Documents and S 2799	ettings/ (2803) 🕵 🕾		Hidden Descriptions	NC
F	/img_xp-sp3-v4.001/vol_vol2/	(4) 🚳 zinelibrary.info	: SESS660e5bd959	Short: /imgxp-sp3-y4.001/yol_yol2/WINDOV	NS



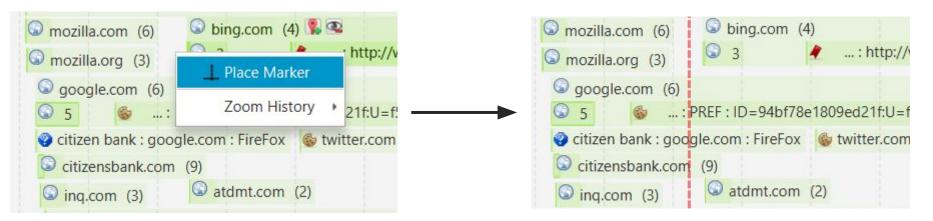






Place guide markers as references you explore

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



	View Mode: 🏨 🕻	Counts 🗮 Det	ails 📃 List	Snapshot Report	🔓 Refresh Vie	iew 🛛 😫 Update D
History 🔶 Back 🔿 Forward						64 eve
Filters Events	Date/Time	Event Type	Description	Known	Tagged	Hash Hit
Apply Default	2005-06-21 00:36:22	M_B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/plug_ins/VDKHome/ENU/VDK10.STC	known		
V Text Filter	2005-06-21 00:36:22	M_B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/plug_ins/VDKHome/ENU/VDK10.STP	known		
ener mie verg	2005-06-21 00:36:22	M_B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/plug_ins/VDKHome/ENU/VDK10.SYD	known		
Hide Known Files	2005-06-21 00:36:22	M_B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/plug_ins/VDKHome/ENU/Vdk10.ing	known		
✓ Data Source	2005-06-21 00:36:22	M_B	/img.xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/plug_ins/VDKHome/ENU/Vdk10.rst	known		
Tags	2005-06-21 00:36:22	M_B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/plug_ins/VDKHome/ENU/acro20.ing	known		
Hash Sets	2005-06-21 00:36:22	M_B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/plug_ins/VDKHome/VDK10.CMP	known		
V Event Type	2005-06-21 00:36:22	M_B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/plug_ins/VDKHome/VDK10.UC	known		
V File System	2005-06-21 00:36:22	M_B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/plug_ins/VDKHome/VDK10.STD	known		
• V Web Activity	2005-06-21 00:36:22	M_B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/plug_ins/VDKHome/VDK10.5YX	known		
	2005-06-21 00:36:22	M_B	/img.xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/plug_ins/VDKHome/VDK10.THD	known		
Misc Types	2006-03-30 12:34:35	in Exif	Canon : Canon EOS-1Ds Mark II : F733Fd01	unknown		
	2006-06-10 00:13:24	M_B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/Tracker/info.gif	known		
	2005-06-10 00:19:04	M_B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/Tracker/add_reviewer.gif	known		
	2006-06-10 00:21:36	M_B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/Tracker/email_all.gif	known		
	2005-06-10 00:24:52	M B	/img xp-sp3-v4.001/vol vol2/Program Files/Adobe/Reader 9.0/Reader/Tracker/email initiator.pif	known		
	2005-06-10 00:29:42	M_B	/img_xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/Tracker/review_email.gif	known		
	2006-06-10 00:30:46	M_B	/img.xp-sp3-v4.001/vol.vol2/Program Files/Adobe/Reader 9.0/Reader/Tracker/review.shared.gif	known		
	2005-06-10 00:32:08	M_B	/img.xp-sp3-v4.001/vol.vol2/Program Files/Adobe/Reader 9.0/Reader/Tracker/review, browser.gif	known		
	2006-06-10 00:33:14	M_B	/img.xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/Tracker/trash.gif	known		
	2005-06-10 00:54:46	M_B	/img.xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/Tracker/reviewers.gif	known		
	2006-06-10 00:57:12	M_B	/img.xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/Tracker/server_lg.gif	known		
	2005-08-04 18:07:52	M.C.	/img.xp-sp3-v4.001/vol_vol2/Documents and Settings/John/My Documents/lang/arabic/المات أغانى غيروز/doc	unknown		
	2005-08-04 18:08:28	M.C.	/img.xp-sp3-v4.001/vol_vol2/Documents and Settings/John/My Documents/lang/arabic/_alkJl ####.doc	unknown		
	2005-08-16 21:08:50	M_B	/img xp-so3-v4.001/vol vol2/Program Files/Adobe/Reader 9.0/Reader/DTemplates/ENU/DefaultID.pdf	known		
	2005-08-16 21:09:20	M_B	/img.xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Reader/IDTemplates/ENU/AdobeID.pdf	known		
	2005-08-25 19:00:33	M_B	/img.xp-sp3-v4.001/vol_vol2/Program Files/Adobe/Reader 9.0/Setup Files/(AC768A96-7AD7-1033-7844-A94000000001)/setup.ini	known		
	2005-09-26 21:37:45	MAC	Jimn vn-sn3-vid 0015/vol vol2/Documents and Settinos/John/My Documents/Jann/ch/SC GR2312 htm	unknown		
	-	_				
		51:02 AM	Jump By: Year 👻 🚺 4 🕨 🕅		Oct 21, 2006 5	5:59:54 AM

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

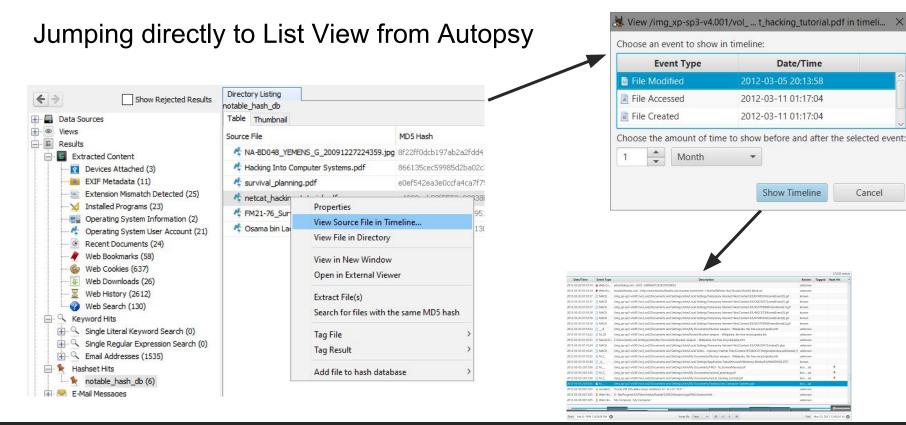


Cancel

Date/Time

Known Tagged Hash Hit

End: Mar 23, 2012 12:42:01



Scenario 2: List View



Tilters	Events	
 Apply 	Default	
✓ Text F	ilter	hacking
Hide k	Known Files	
🔻 🔽 Data S	Source	

Adding a text
filter, reduces
the view to 20
events

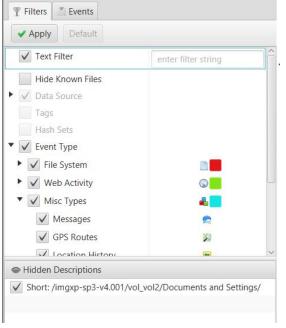
Date/Time	Event Type	Description	Known	Tagged	Hash Hit
012-03-03 01:02:27	📓 Web His	google.com : http://www.google.com/#hl=en&sclient=psy-ab&q=hackin =ebada0e4be87c9aa&biw=800&bih=509 : hacking guide - Google Search	unknown		
2012-03-03 01:02:27	Web Sea	hacking guide : google.com : Chrome	unknown		
2012-03-03 01:02:30	🗵 Web His	$google.com: http://www.google.com/url?sa=t&rct=j&q=hacking\%20gu \dots q9rT8qGJKTX0QHIs6jJBg&usg=AFQjCNFICbYFIOcRZYq4FVp56EuG9CSDkg: http://www.google.com/url?sa=t&rct=j&q=hacking\%20gu \ http://www.google.com/url?sa=t&rct=j&q$	unknown		
2012-03-03 01:02:30	Web Sea	hacking guide : google.com : Chrome	unknown		
2012-03-03 01:02:32	🗵 Web His	$google.com: http://www.google.com/url?sa=t&rct=j&q=hacking\%20gu q9rT8qGJKTX0QHIs6jJ8g&usg=AFQjCNHarEwAfXISJ2oiv_O7moFq5pm5ig: http://www.google.com/url?sa=t&rct=hacking\%20gu q9rT8qGJKTX0QHIs6jJ8g&usg=AFQjCNHarEwAfXISJ2oiv_O7moFq5pm5ig: http://www.google.com/url?sa=t&rct=hacking\%20gu q9rT8qGJKTX0QHIs6jJ8g&usg=AFQjCNHarEwAfXISJ2oiv_O7moFq5pm5ig: http://www.google.com/url?sa=t&rct=hacking\%20gu q9rT8qGJKTX0QHIs6jJ8g&usg=AFQjCNHarEwAfXISJ2oiv_O7moFq5pm5ig: http://www.google.com/url?sa=t&rct=hacking\%20gu q9rT8qGJKTX0QHIs6jJ8g&usg=AFQjCNHarEwAfXISJ2oiv_O7moFq5pm5ig: http://www.google.com/url?sa=t&rct=hacking\%20gu q9rT8qGJKTX0QHIs6jJ8g&usg=AFQjCNHarEwAfXISJ2oiv_O7moFq5pm5ig: http://www.google.com/url?sa=t&rct=hacking\%20gu q9rT8qGKTAWAfXISJ2oiv_AfXI$	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.utmcsr=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%20 and%20 Settings/John/My%20 Documents/Hacking%20 Into%20 Computer%20 Systems.pdf: 0.00000000000000000000000000000000000	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	🛅В	/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		
	A_	/imq_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

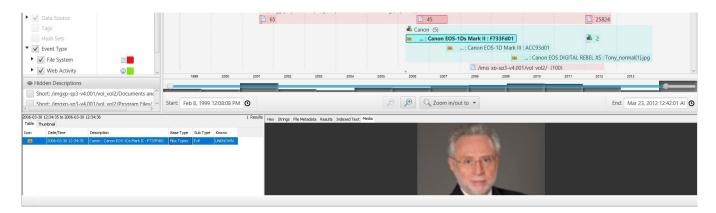
Filter on: Description, known status, event type,data sources, tags, hash sets



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

٠



