



Collaborative Autopsy: Enterprise Open Source Forensics

Richard Cordovano

October 28, 2015 | Westin Washington Dulles, Herndon, VA

The Wonderful Present



- The number of devices to be examined in digital forensics cases is increasing
- The devices are larger...much larger
- Examiners need to collaborate to get the work done quickly and efficiently...but how?

A Solution?



- Break a large case up into sets of images
- Assign multiple people to the case
- Each person works on one set of images with a single-user tool
- Merge the results when all analysis is complete

Not Ideal



- The work gets done faster but...
 - Each person is working in isolation
 - Tagged/bookmarked results are scattered across the case files for each person
 - Merging results is not easy
 - Merging results might need to be done more than once

Need a collaborative environment



- In a collaborative system...
 - Everyone can see all of the results in something like real time
 - No merging of results required
 - Single, unified report generated at any time
- Collaborative systems exist but they cost a lot of money
 - How many have this? How many want this but cannot afford it?



Good News!



- Collaboration features are included in the capabilities Basis has added to a "custom Autopsy" for one of our clients
- The customer approved release of these features to the community
- So Autopsy 4.0 is the advent of "collaborative" Autopsy!
 - Same Autopsy interface, configured to use centralized data and services
- So what did we do, exactly?



Starting Point: Autopsy 3





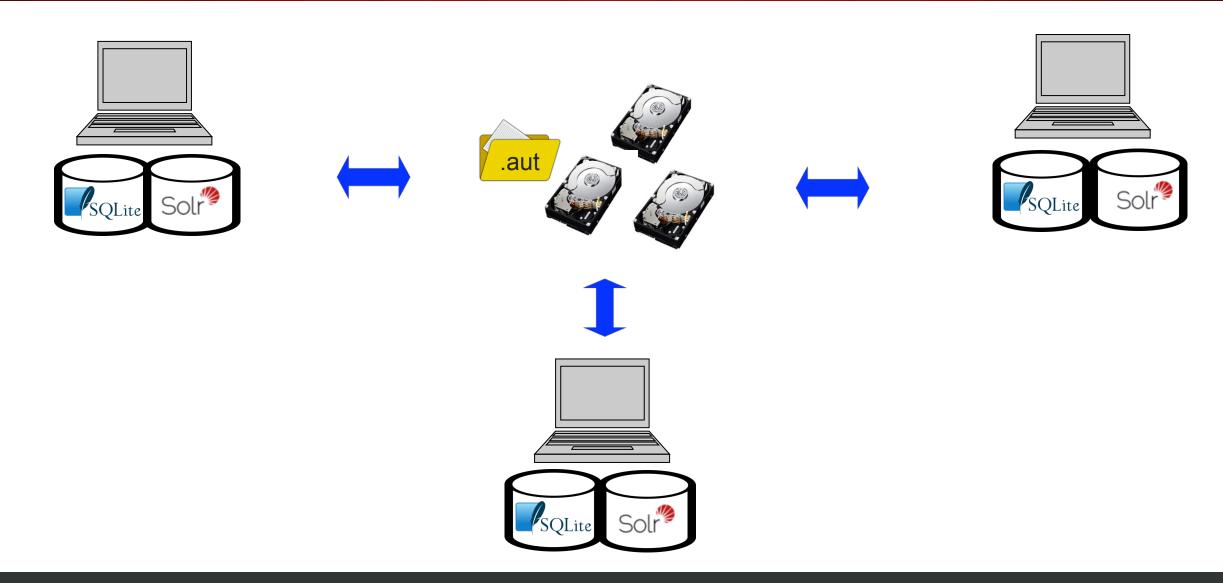






Step 1: Add Centralized Storage





New Concept: Multi-User Case Folders



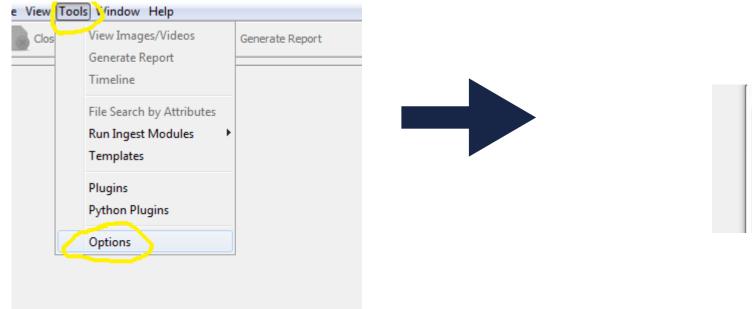
A. Name . ۰. Name Cache host1 Export host2 Log host3 ModuleOutput Reports host4 Temp host5 autopsy.db case.aut case.aut

Multi-user case folder

Single-user case folder

10/28/2015







Store Multi-User Case Files on a File Share

Steps	Case Info	
Case Info Additional Information		
	Enter New Case Information:	
	Case Name: collaboration-1]
	Base Directory: \\file-server-1\cases	Browse
	Case data will be stored in the following directory:	
	\\file-server-1\cases\collaboration-1	
	Single-user Multi-user	
	1	
	< Back Next > Finish Cancel	Help

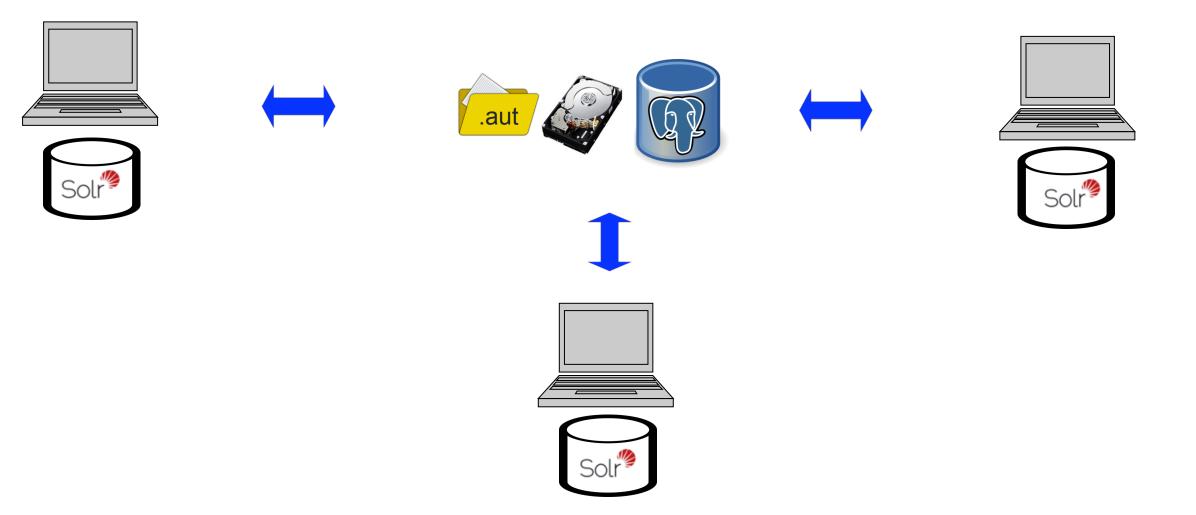
Store Multi-User Images on a File Share



🐇 Add Data Source	22
 Enter Data Source Information Configure Ingest Modules Add Data Source 	Enter Data Source Information wizard (Step 1 of 3) Select source type to add: Image File Browse for an image file: Image File Image Select the input timezone: (GMT-5:00) America/New_York Please select the input 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 input data, extract volume and file system data, and populate a local database.
	< Back Next > Finish Cancel Help

Step 2: Add a Case Database Server





#OSDFCon

About Multi-User Case Databases



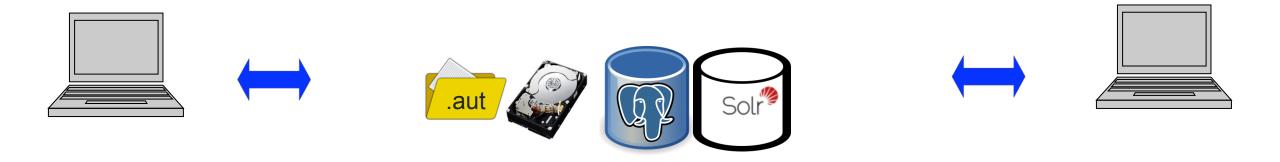
- Individual case database is still small:
 - Schema is identical to that of singe-user (SQLite) in substance
 - Stores file metadata gleaned by the SleuthKit
 - Stores artifact metadata produced by ingest modules
- Still one per case, so it still scales well
 - Add a time stamp suffix to avoid name collisions
- PostgreSQL
 - Open source, enterprise-grade database for free!

Database Settings



V		8				-?	*	
Auto	opsy I	Multi-user	Keyword Searc	h Hash Database	File Extension Mismatch	File Types	Interesting Files	Imag
	V Enal	blo Multi u	oor cocco. Fill in	a all values				
	/ Ena	ble Multi-u	ser cases Fill ir	n all values			~	
	_	ble Multi-u base Sett		n all values		_(Test	
	Datal	base Sett		n all values			Test	
	Datal	base Sett	tings IP Address	n all values			Test	
	Datal Host	base Sett tname or	tings IP Address	n all values			Test	

Step 3: Add a Centralized Solr Instance









#OSDFCon

ASIS

B

Single-User Solr vs Multi-User Solr



- Single-user case Solr instance
 - One "core" (index) per case
 - Stored in case folder
 - Solr runs in web server started when Autopsy starts up
- Multi-user case Solr instance
 - One "core" (index) per case
 - Stored in case folder
 - Solr runs on server
 - Add a time stamp suffix to core name avoid name collisions
- Still free and open source!

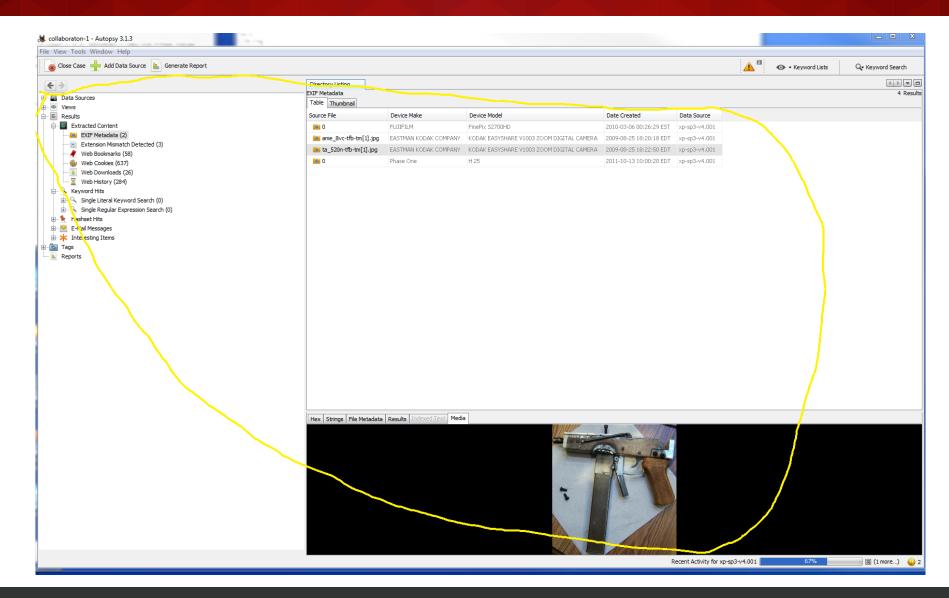
Solr Settings





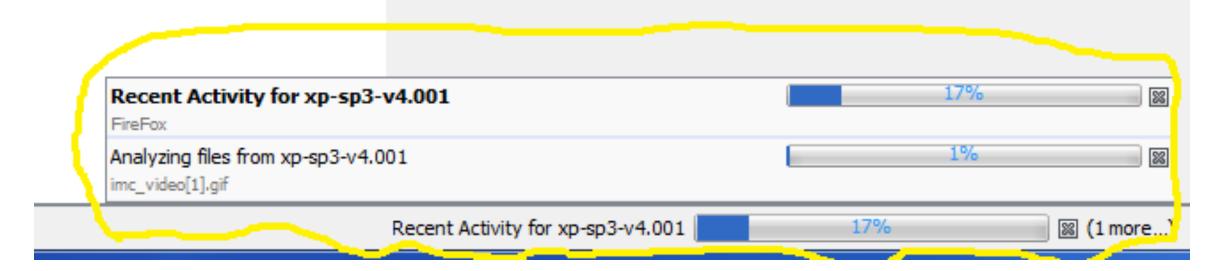
What's Missing? How about this...





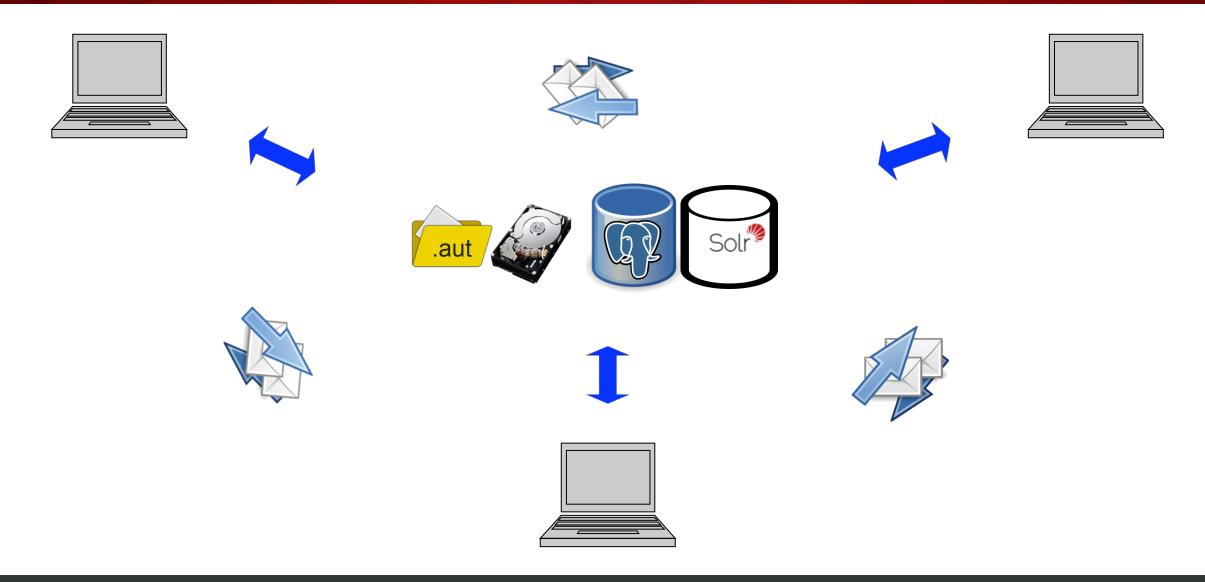
And this...





Step 4: Add Messaging





#OSDFCon

About Messaging



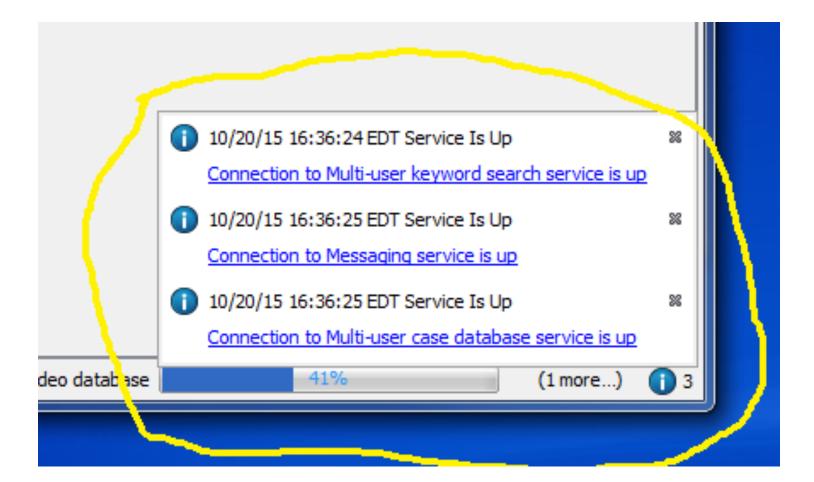
- Autopsy tree updates as images, files, artifacts added to case
 - Bonus: Directory tree no longer opens and closes as things are added!
- Ingest progress bars for ingest by collaborators
 - One per ingest
 - Indeterminate
 - Show host name
- Implemented using Apache ActiveMQ
 - Free and open source!



lostname or IP Address	
Port Number	
Jser Name	
Password	

Step 5: Add Service Monitoring





About Service Monitoring



- Services are checked when a multi-user case is opened
- Services are checked every few minutes thereafter
 - Up and Down messages
- If the PostgreSQL server or the Solr server cannot be reached
 - Ingest won't start
 - Ingest in process will auto-cancel (will probably see some error messages from ingest modules database errors get batched and packaged as notifications)

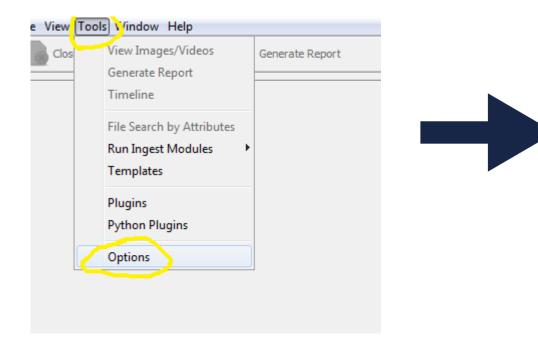
Setting Up Collaborative Autopsy



- Step 1: Download and install Autopsy 4.0
- Step 2: Decide where to centralize your case folders and images
- Step 3: Install and configure PostgreSQL, Solr, and ActiveMQ
 - All free and open source!
 - A few configuration details are in the Autopsy 4.0 documentation
 - We recommend giving Solr its own machine with plenty of RAM, if possible
- Step 4: Point Autopsy 4.0 instances at the above
- Step 5: Collaborate!

Point at Services





2 😵 🔍 📄	-	-?	*			Q Filter (Ctrl-
topsy Multi-user Keyword Search Hash Databas	e File Extension Mismat	tch File Types II	nteresting Files	mage / Video Gal	General Appearan	ce
Enable Multi-user cases Fill in all values						
			\sim			
Database Settings		(Test			
Hostname or IP Address				1		
Port Number						
User Name						
Password						
				_ <u>}</u>		
Solr Settings		(Test			
Hostname or IP Address			\smile			
Port Number				 		
ActiveMQ Message Service Settings		1	Test			
Hostname or IP Address		· · · ·				
Port Number						
User Name						
Password						

#OSDFCon

Create a Multi-User Case



Steps	Case Info
 Case Info Additional Information 	Enter New Case Information:
	Case Name: collaboration-1
	Base Directory: \\file-server-1\cases Browse
	Case data will be stored in the following directory:
	\\file-server-1\cases\collaboration-1
	Single-user Multi-user
	1
	< Back Next > Finish Cancel Help

Add a Data Source (Image)



teps	Enter Data Source Information wizard (Step 1 of 3)
 Enter Data Source Information Configure Ingest Modules Add Data Source 	Select source type to add: Image File Browse for an image file: Utile-server-1\images Please select the input timezone: (GMT-5:00) America/New_York Please select the input timezone: (GMT-5:00) America/New_York (faster results, although some data will not be searched)
	Press 'Next' to analyze the input data, extract volume and file system data, and populate a local database.

Configure and Run Ingest Modules



ps	Configure Ingest Modules wizard (Step 2 of 3)
Enter Data Source Information Configure Ingest Modules Add Data Source	Configure the ingest modules you would like to run on this data source.
	 Recent Activity Hash Lookup File Type Identification Embedded File Extractor Exif Parser Exif Parser Exit Parser Email Parser Extension Mismatch Detector E01 Verifier Android Analyzer Interesting Files Identifier PhotoRec Carver
	Select All Deselect All Performs file indexing and periodic sear Advanced Process Unallocated Space Advanced

Other Examiners Join In





Analyze and Report



File View Tools Window Help	
Close Case 🚽 Add Data Source 🚡 Generate Report	
< >	
🕀 🖳 Data Sources	
🗄 🐵 Views	
🖶 🖷 🖾 Results	
Extracted Content	
Devices Attached (3)	
EXIF Metadata (19)	
Extension Mismatch Detected (56)	
Operating System Information (2)	

Known Limitations

BASIS

- No shared configuration yet
 - We have an initial version of this in "custom Autopsy", but there are details to iron out for a community release
- Results and tags are not associated with a user
- Results are not associated with a data source (image)
 - Can become confusing if a case is large
- Some things in the case folder might be better stored higher in the folder hierarchy (e.g., reports, exports, Solr core)
- Single-user to multi-user case conversion is not publicly fullysupported at this time
- Ingest status for collaborators is not that detailed

Training and Support



- Basis provides commercial support for labs using Autopsy that want more than community support
 - We can build a custom app on top of Autopsy for you!
- Basis offers training, but it does not yet cover the collaborative features

The End/Questions?





