6th Annual
#OSDFCon
OPEN SOURCE DIGITAL FORENSICS CONFERENCE

BASIS TECHNOLOGY

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

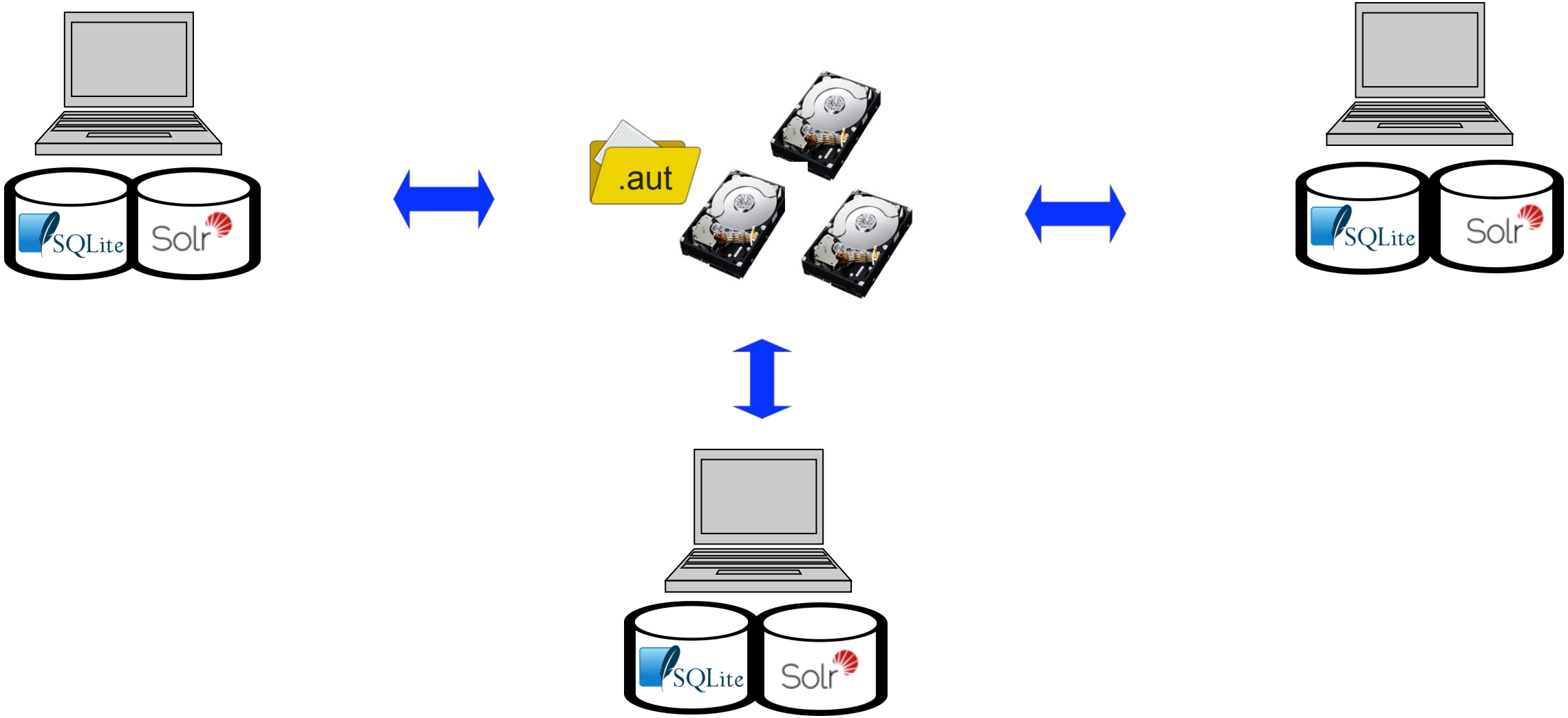
- In a collaborative system…
  - Everyone can see all of the results in something like real time
  - No merging of results required
  - Single, unified report generated at any time
- Collaborative systems exist but they cost a lot of money
  - How many have this? How many want this but cannot afford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

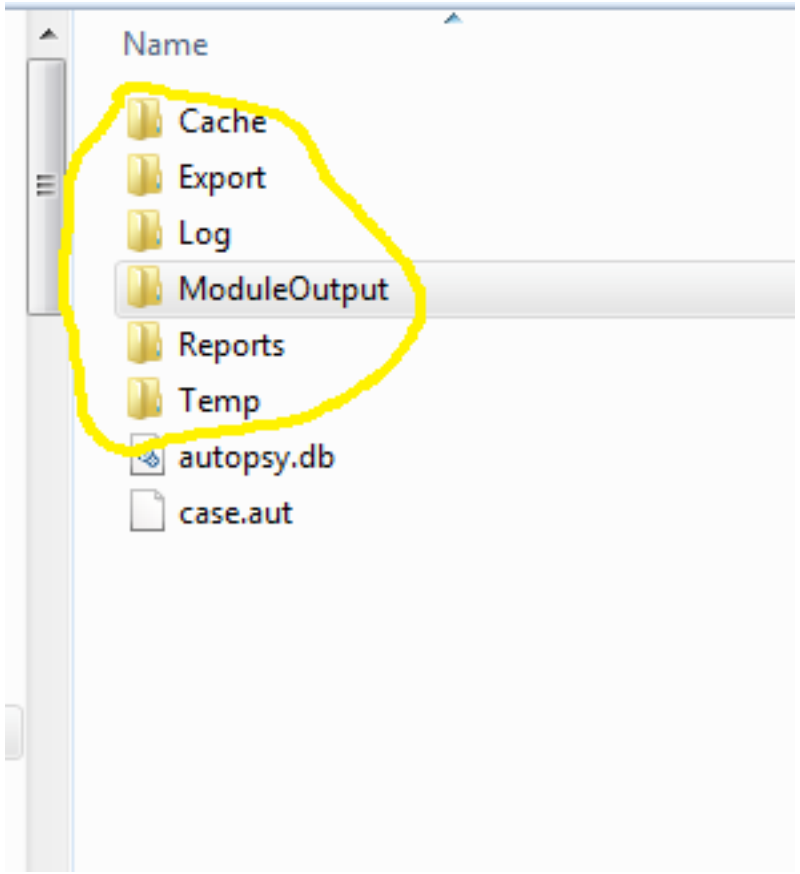
Starting Point: Autopsy 3

Step 1: Add Centralized Storage

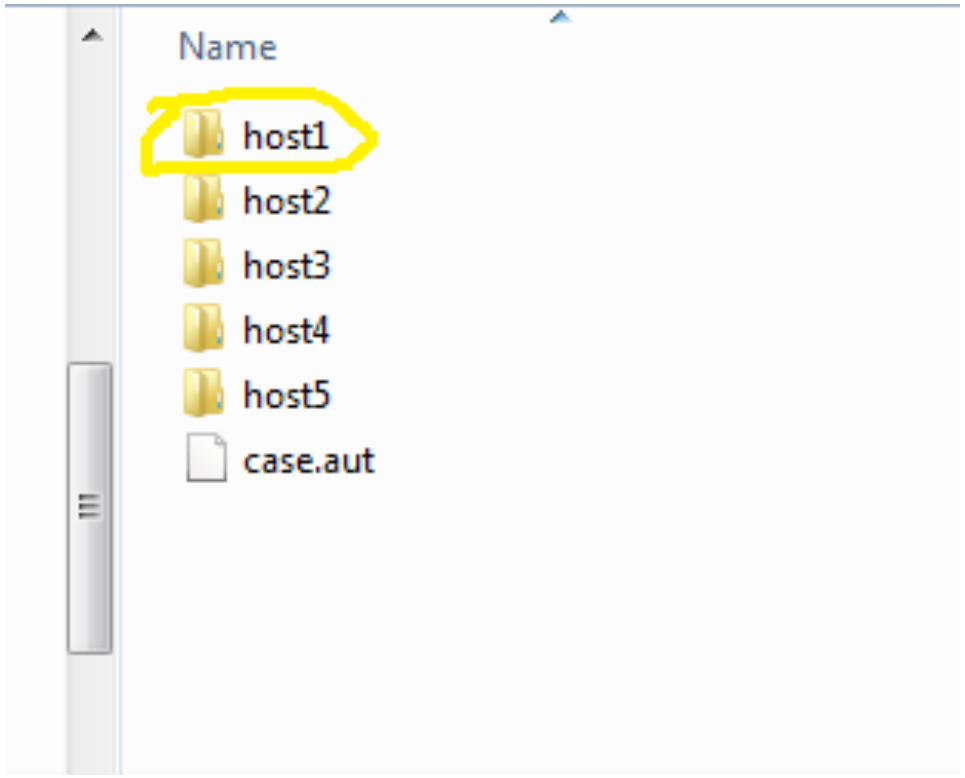


New Concept: Multi-User Case Folders

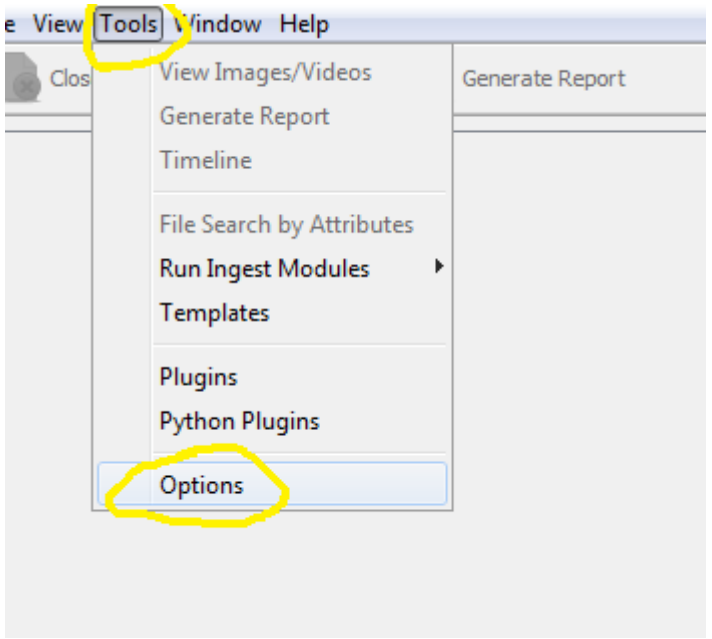
Single-user case folder

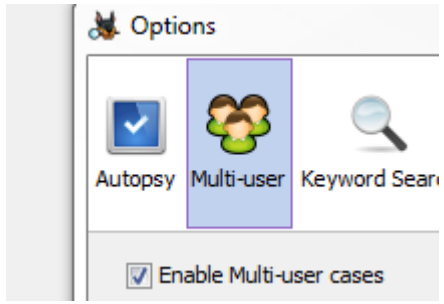


Multi-user case folder

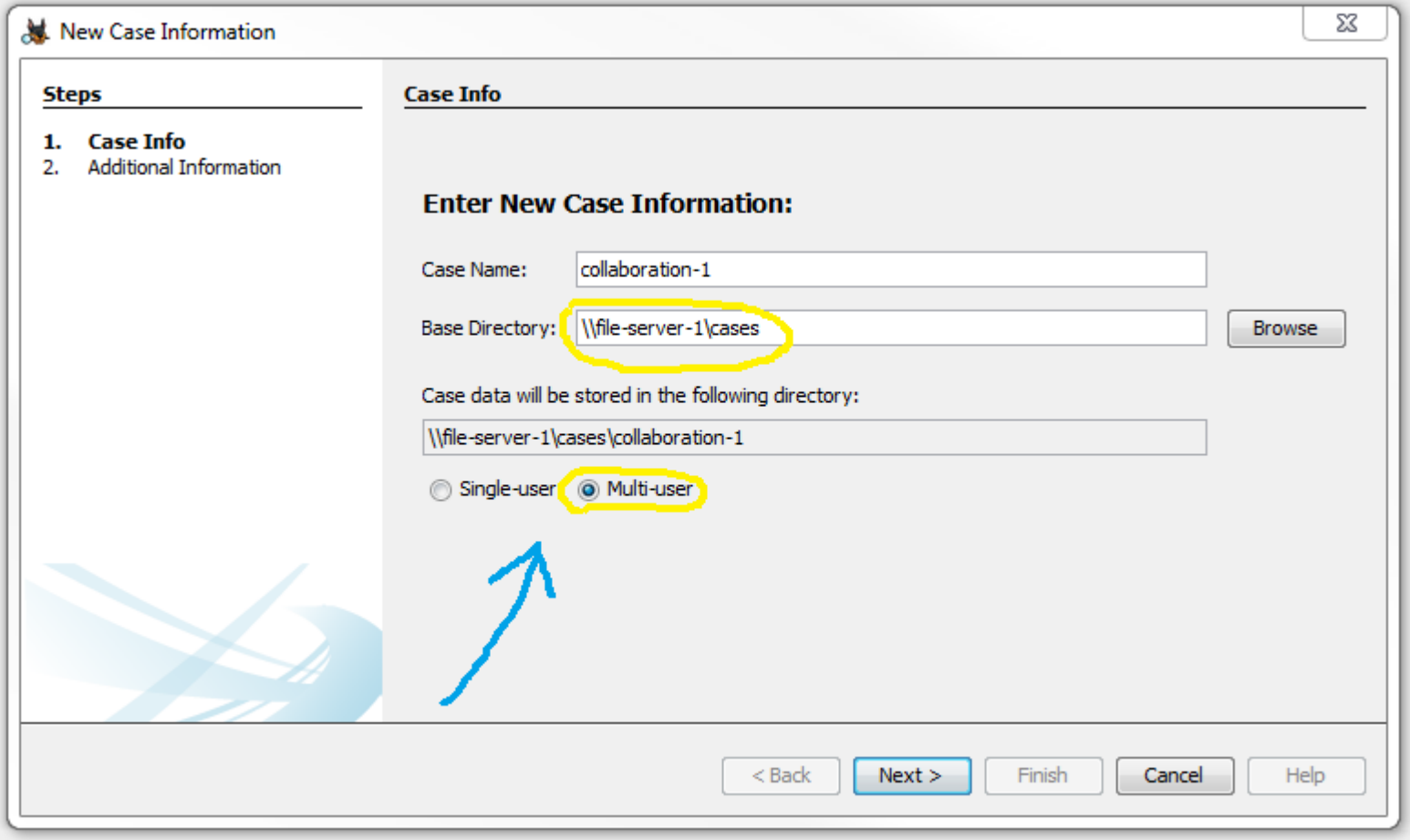


Enable Multi-User Cases

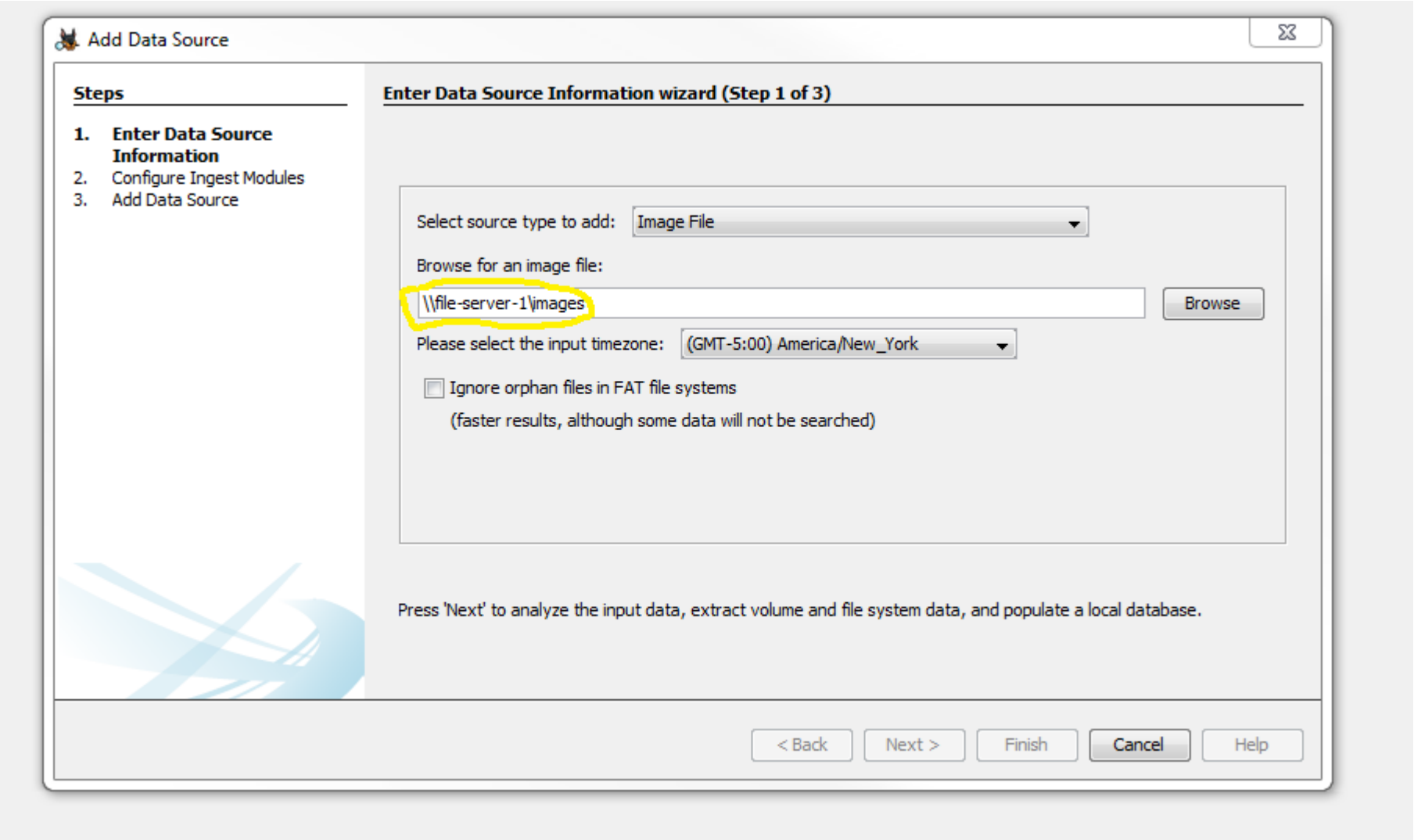




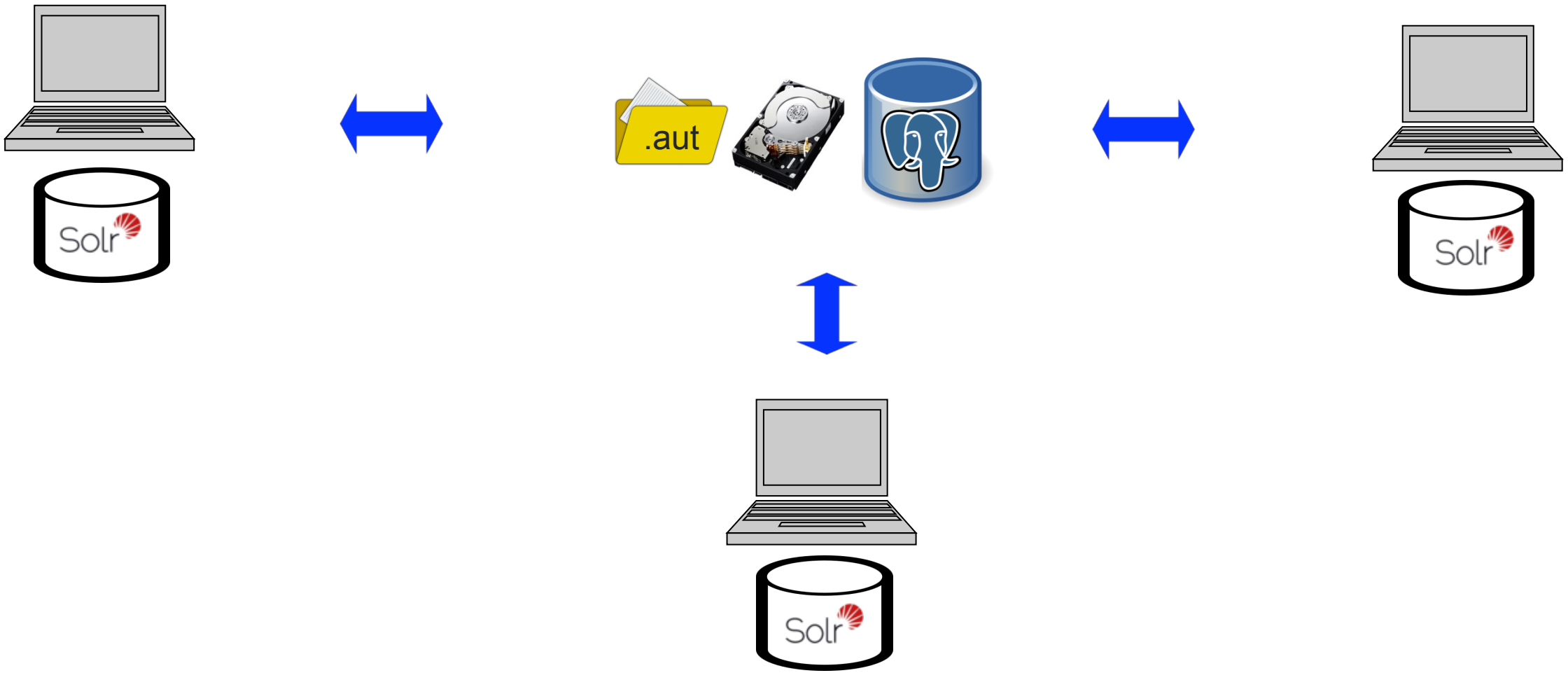
Store Multi-User Case Files on a File Share



Store Multi-User Images on a File Share



Step 2: Add a Case Database Server

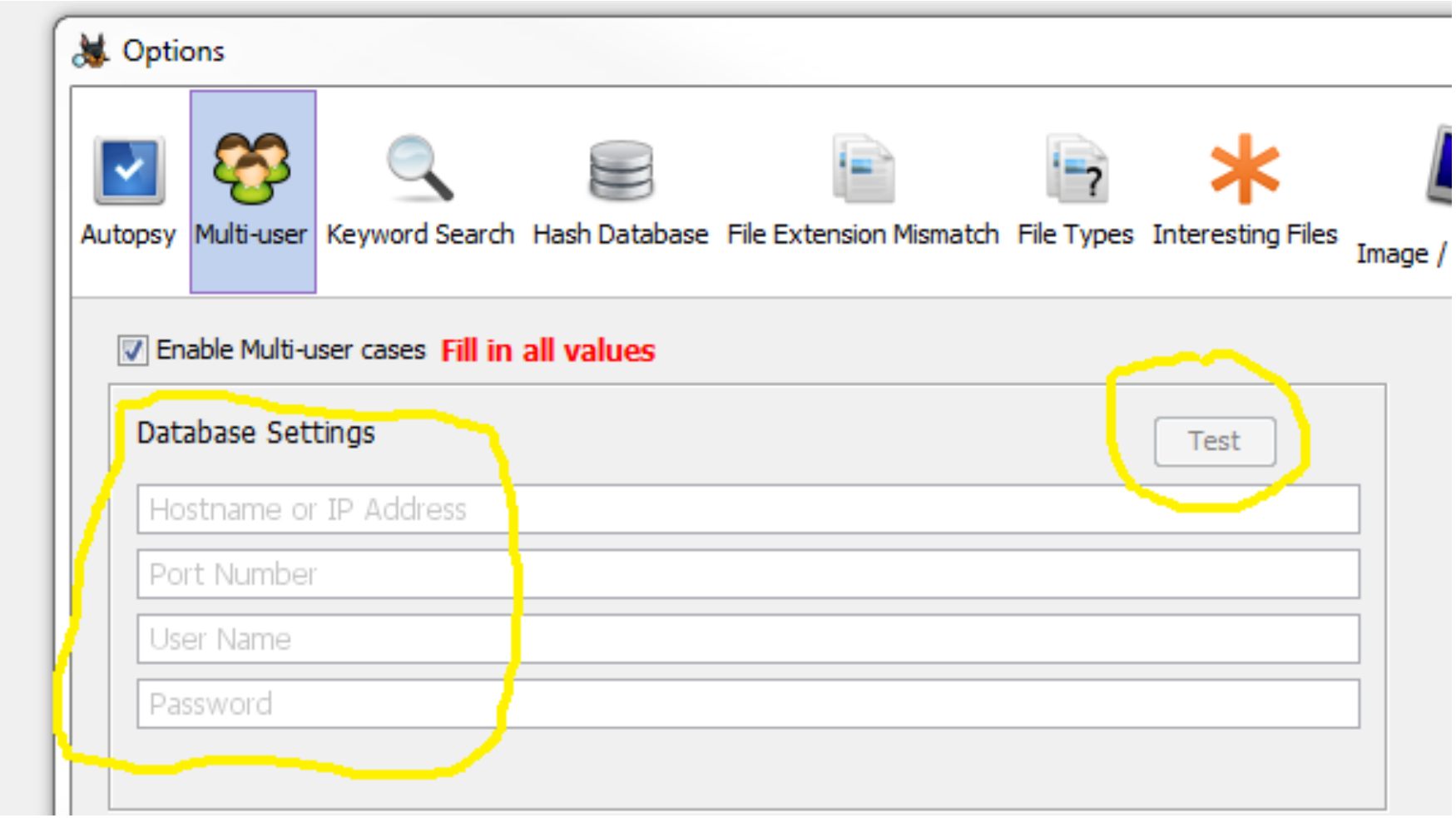


About Multi-User Case Databases

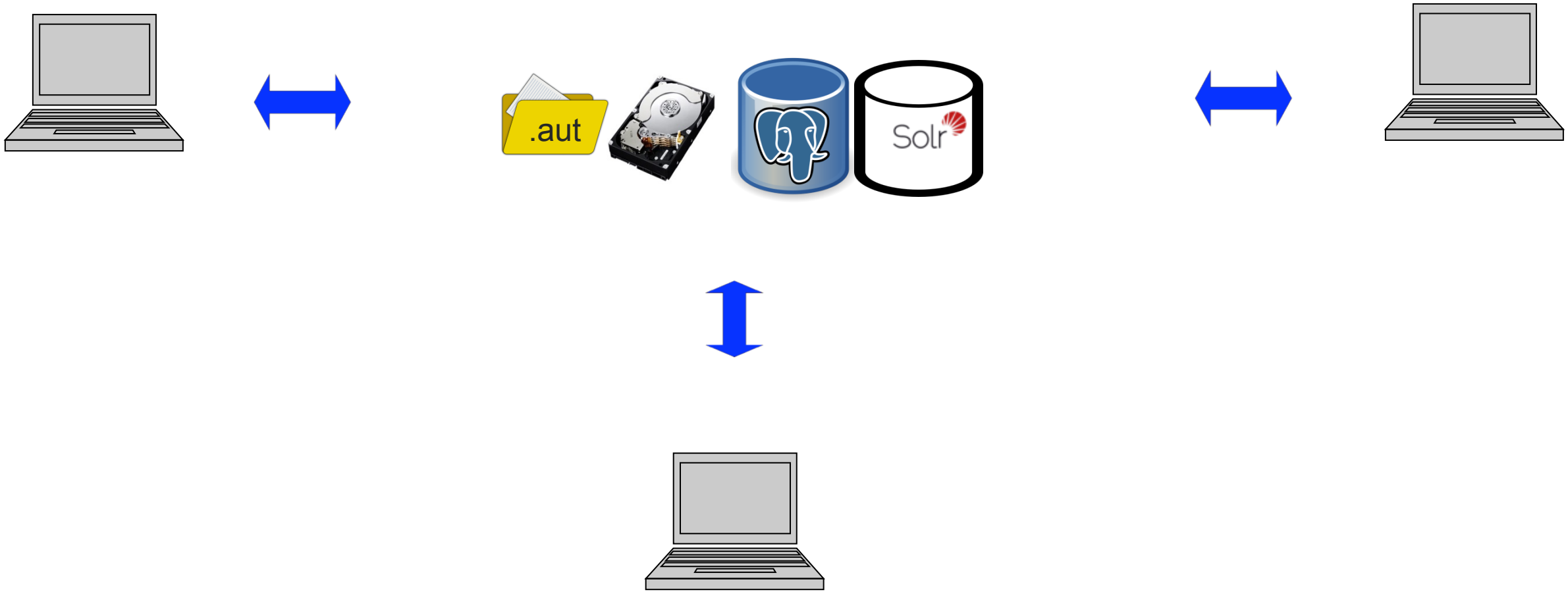
BASIS TECHNOLOGY

- 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



Step 3: Add a Centralized Solr Instance



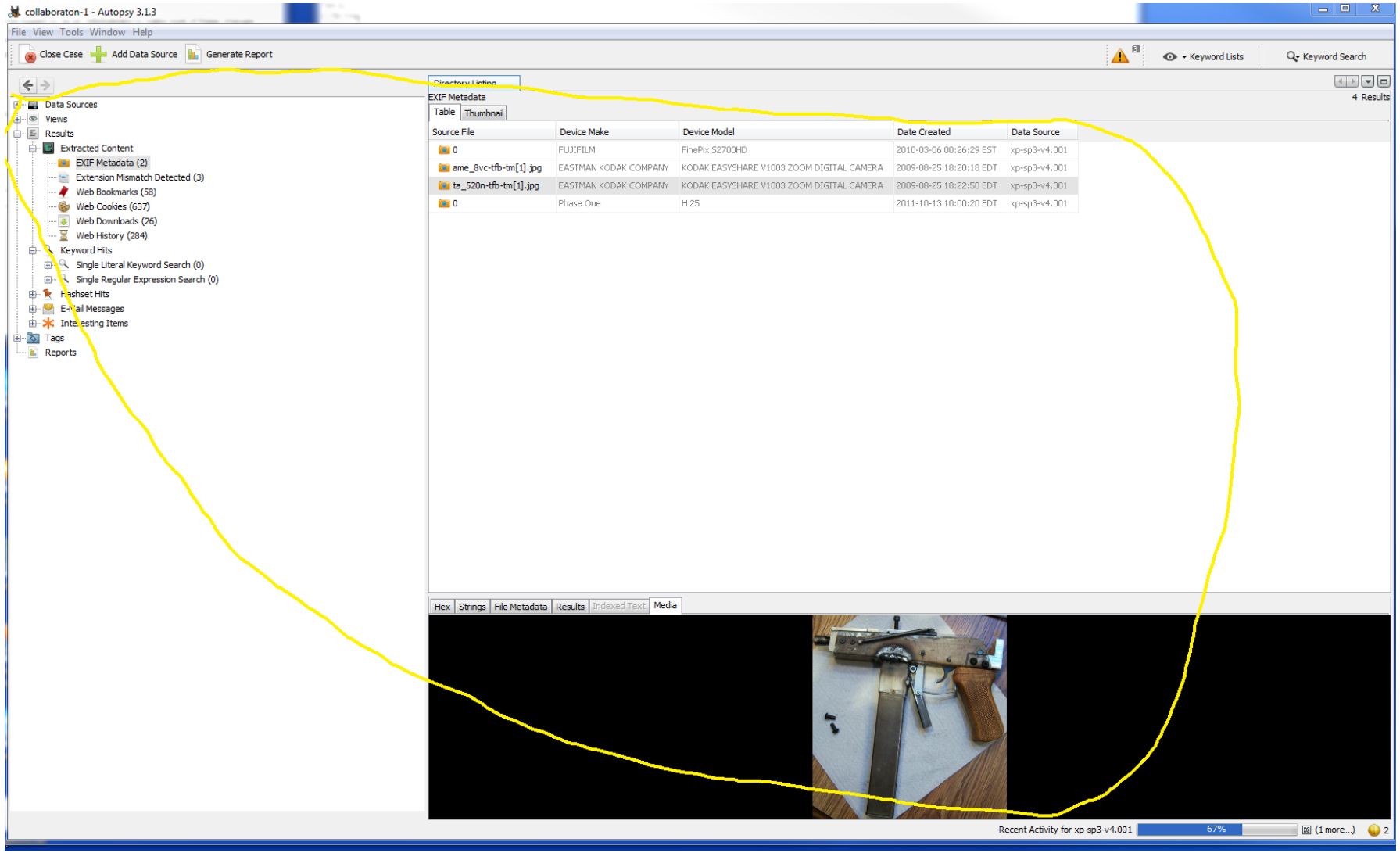
Single-User Solr vs Multi-User Solr

BASIS TECHNOLOGY

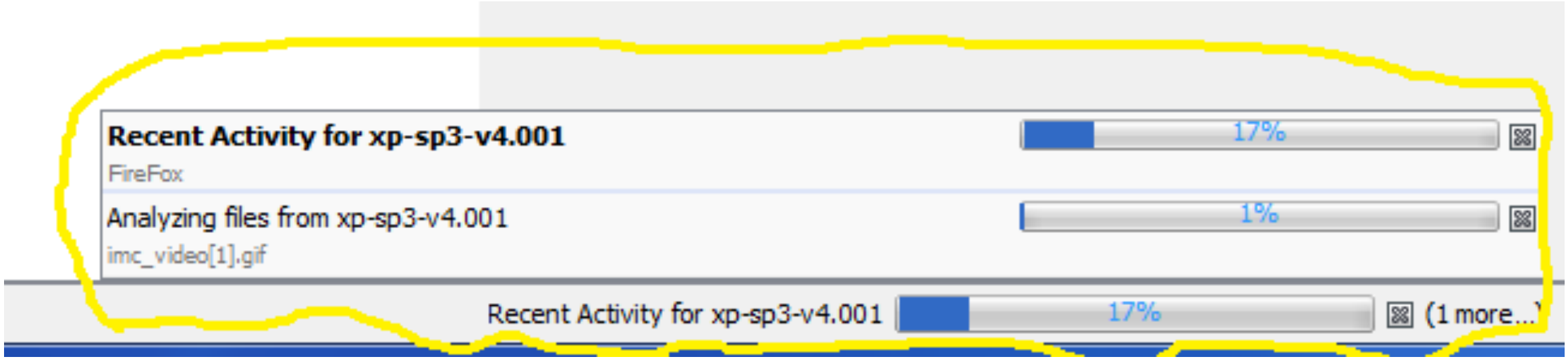
- Single-user case Solr instance
  - One “core” (index) per case
  - Stored in case folder
  - Solr runs in web server started when Autopsy starts up
- Multi-user case Solr instance
  - One “core” (index) per case
  - Stored in case folder
  - Solr runs on server
    - Add a time stamp suffix to core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

Solr Settings

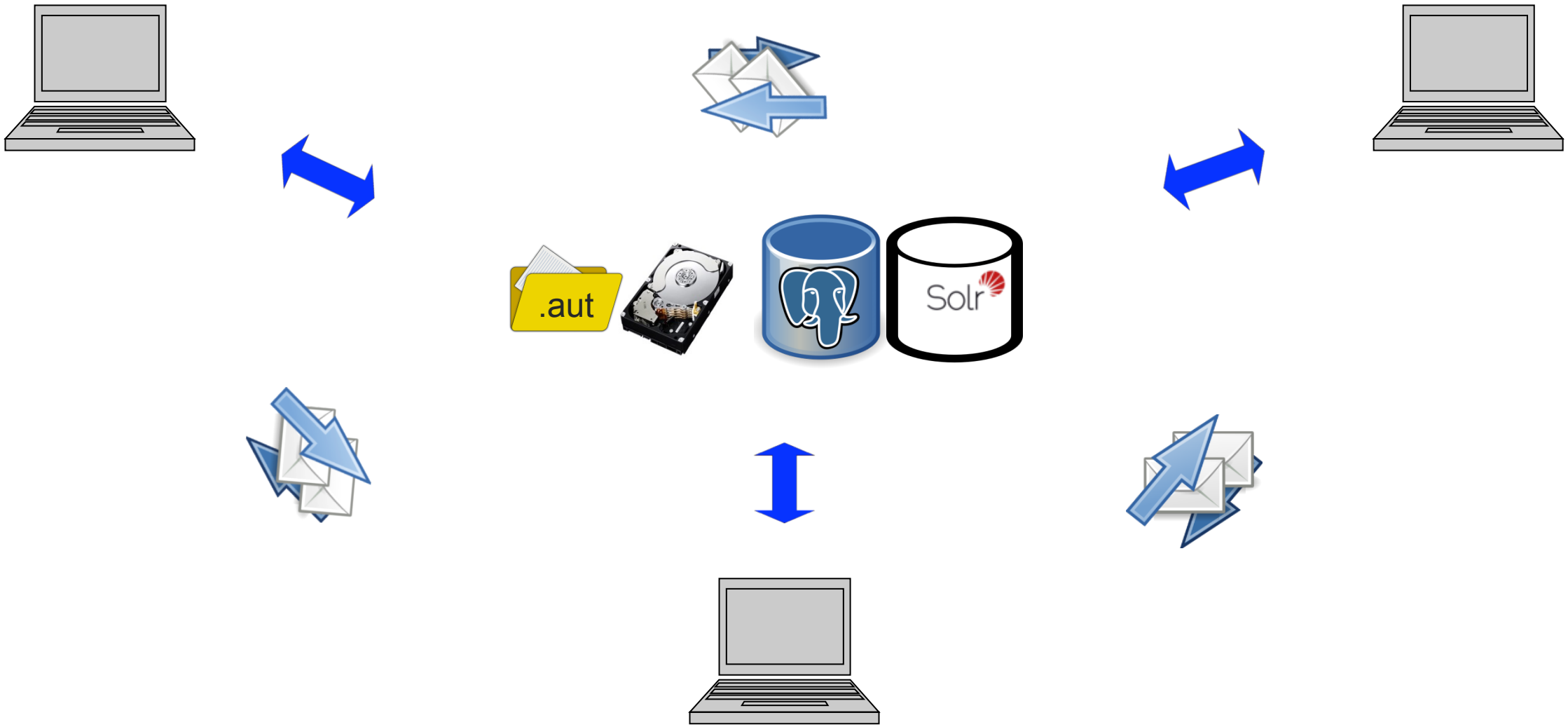
What's Missing? How about this…



And this…


Recent Activity for xp-sp3-v4.001
FireFox
17%
Analyzing files from xp-sp3-v4.001
imc_video[1].gif
1%
Recent Activity for xp-sp3-v4.001
17%
(1 more...)

Step 4: Add Messaging

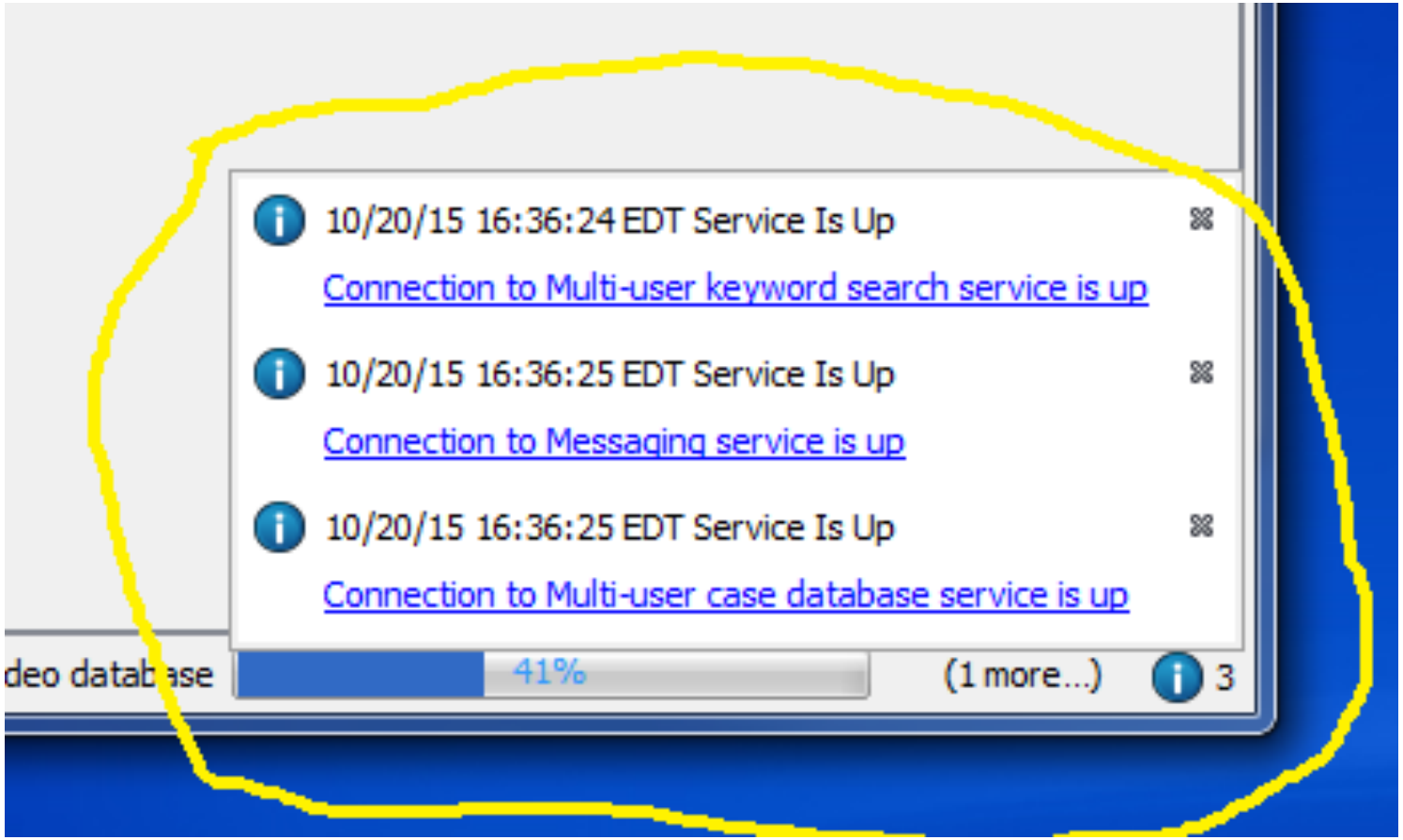


About Messaging

- 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!

Messaging Settings

Step 5: Add Service Monitoring



About Service Monitoring

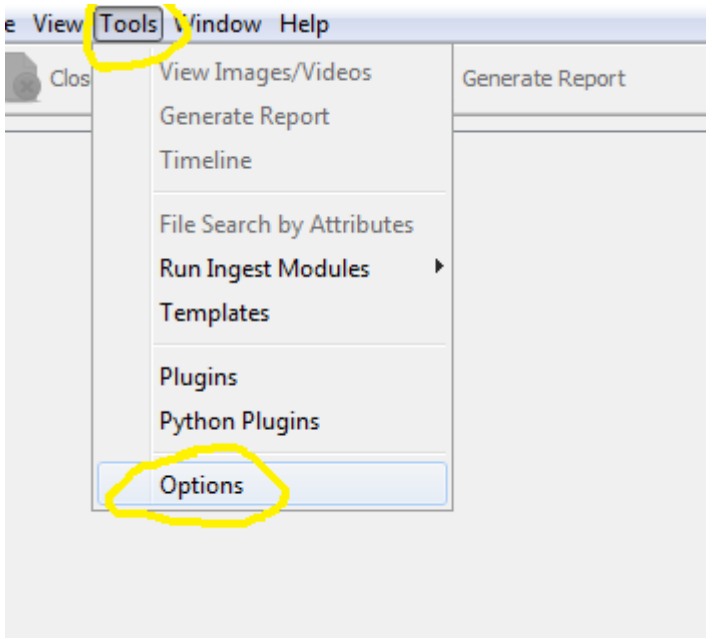
- Services are checked when a multi-user case is opened
- Services are checked every few minutes thereafter
  - Up and Down messages
- If the PostgreSQL server or the Solr server cannot be reached
  - Ingest won't start
  - Ingest in process will auto-cancel (will probably see some error messages from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

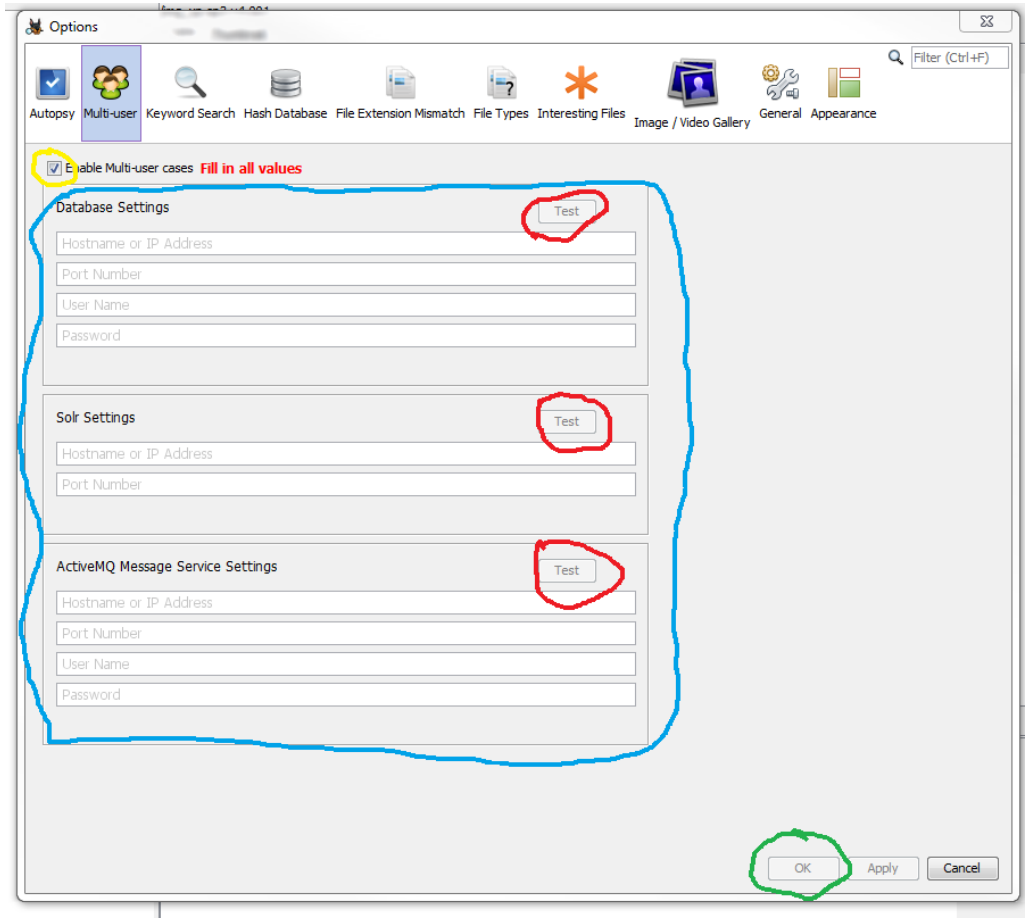
Setting Up Collaborative Autopsy

BASIS TECHNOLOGY

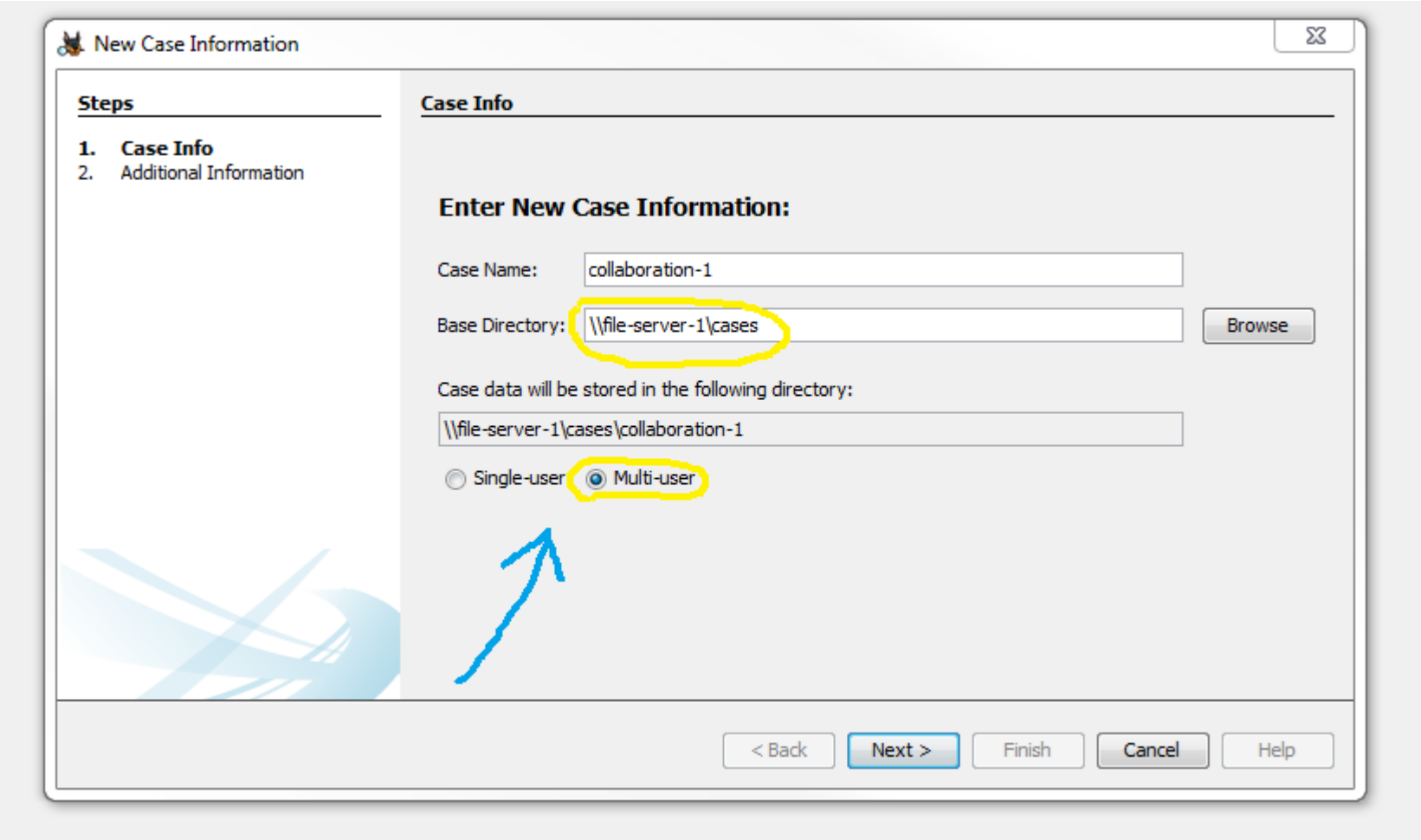
- Step 1: Download and install Autopsy 4.0
- Step 2: Decide where to centralize your case folders and images
- Step 3: Install and configure PostgreSQL, Solr, and ActiveMQ
  - All free and open source!
  - A few configuration details are in the Autopsy 4.0 documentation
  - We recommend giving Solr its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

Point at Services

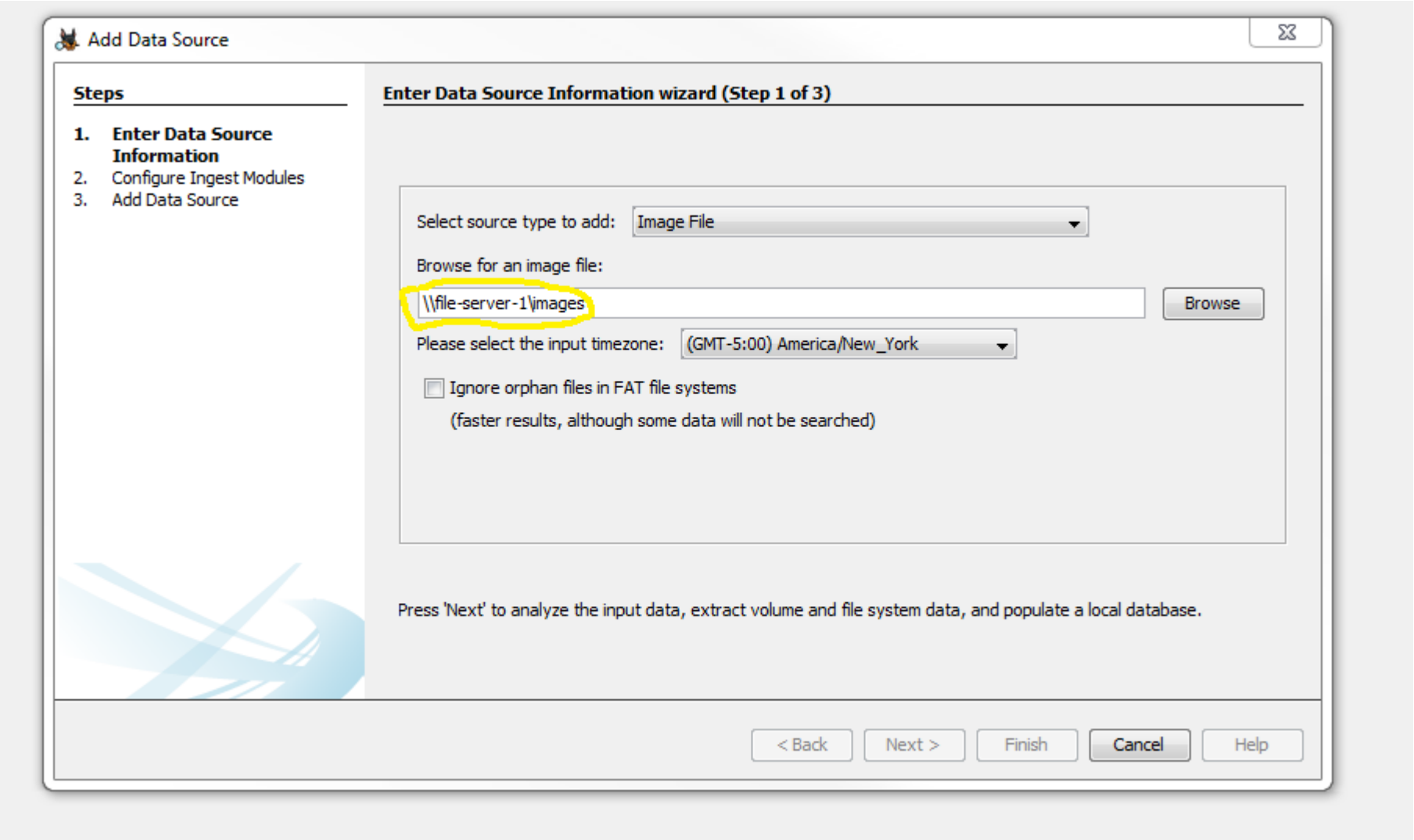




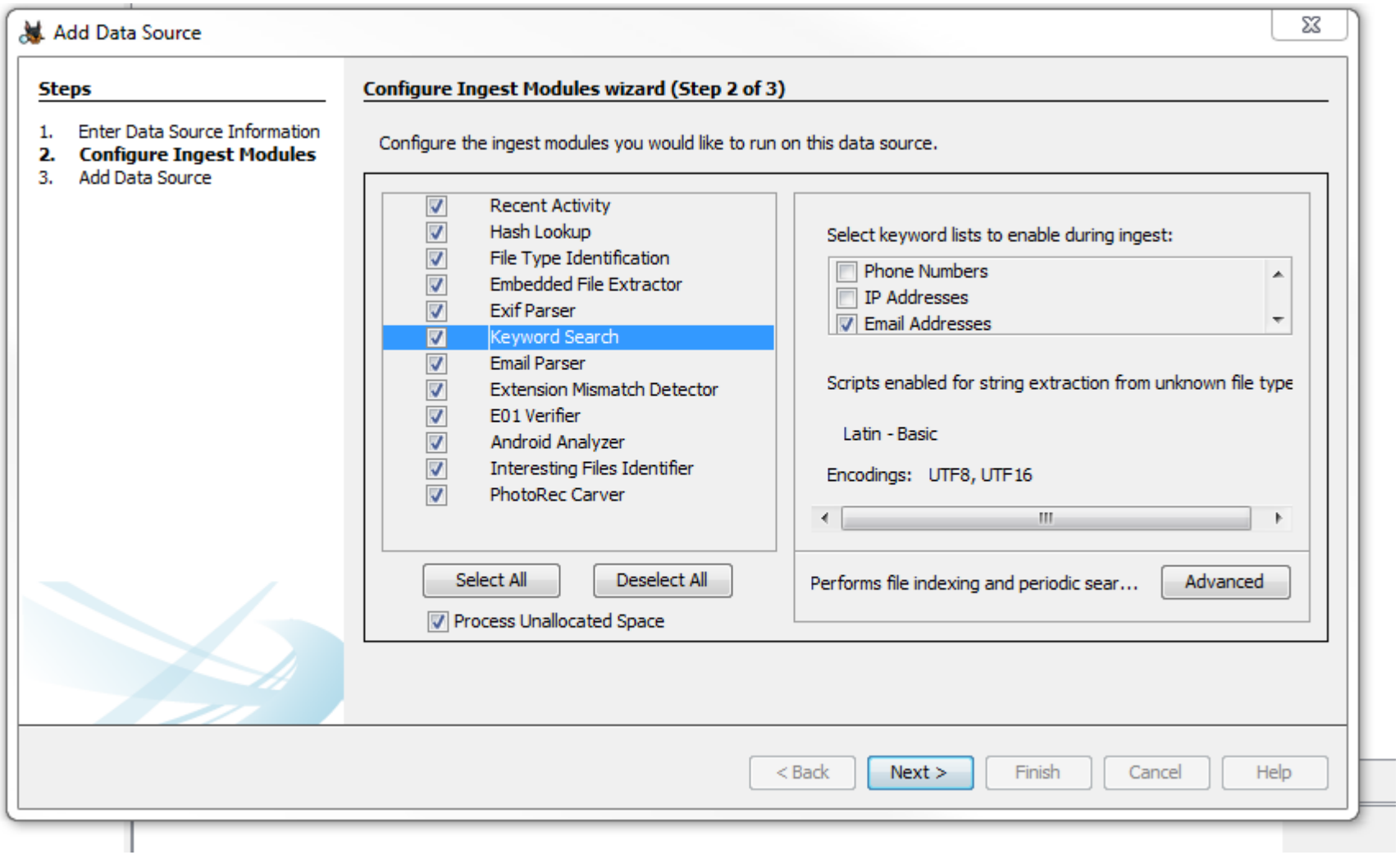
Create a Multi-User Case



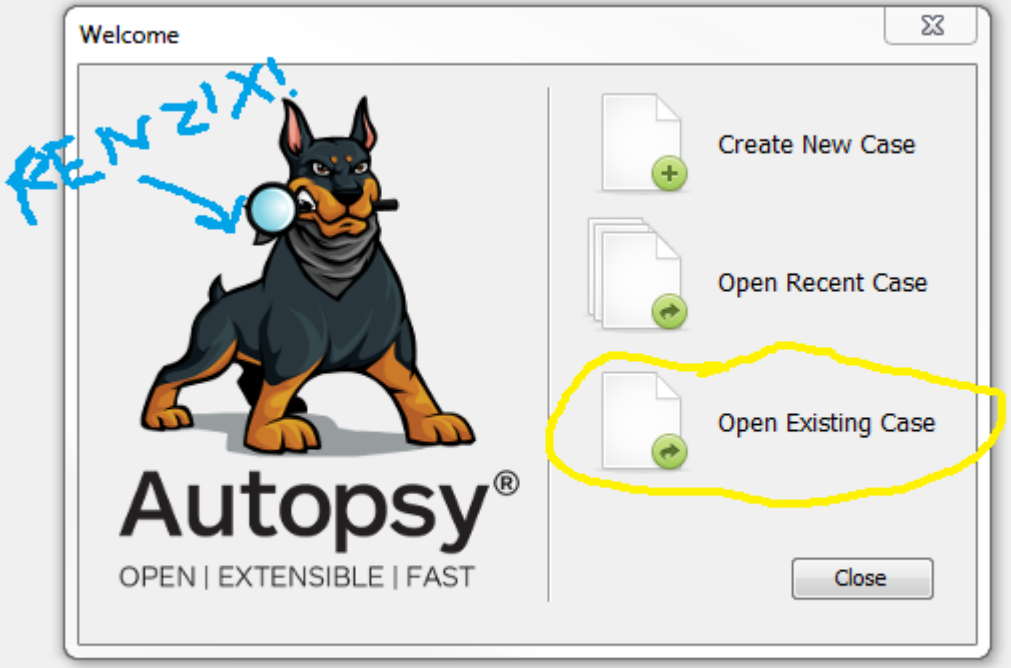
Add a Data Source (Image)



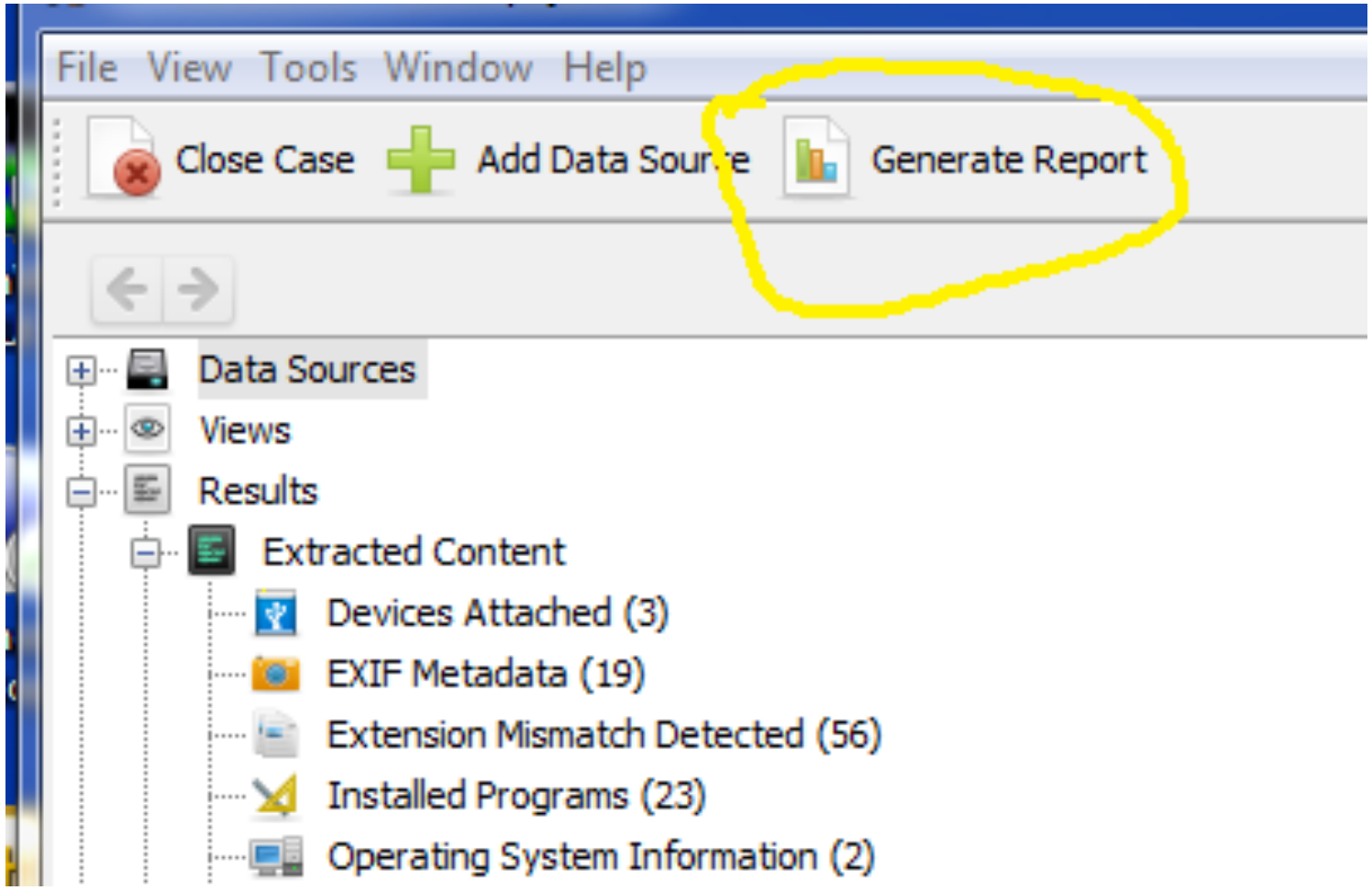
Configure and Run Ingest Modules



Other Examiners Join In



Analyze and Report



Known Limitations

- 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 fully-supported 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?