Collaborative Autopsy: Enterprise Open Source Forensics

Richard Cordovano
• 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?
• 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?

Good News!
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

- Case Name: collaboration-1
- Base Directory: file-server-1\cases

Case data will be stored in the following directory:
file-server-1\cases\collaboration-1

Choose either Single-user or Multi-user.
Store Multi-User Images on a File Share
Step 2: Add a Case Database Server
About Multi-User Case Databases

• Individual case database is still small:
  • Schema is identical to that of single-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

Options

Autopsy Multi-user Keyword Search Hash Database File Extension Mismatch File Types Interesting Files Image /

Enable Multi-user cases Fill in all values

Database Settings

Hostname or IP Address
Port Number
User Name
Password

Test
Step 3: Add a Centralized Solr Instance
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

Hostname or IP Address

Port Number

Test
What’s Missing? How about this…
And this…
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

ActiveMQ Message Service Settings

- Hostname or IP Address
- Port Number
- User Name
- Password

Test
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
Create a Multi-User Case

Enter New Case Information:

Case Name: collaboration-1
Base Directory: \file-server-1\cases

Case data will be stored in the following directory:
\file-server-1\cases\collaboration-1

Single-user [ ] Multi-user [ ]
Add a Data Source (Image)

Select source type to add: Image File

Browse for an image file: \file-server-1\Images

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.
Configure and Run Ingest Modules

Configure Ingest Modules wizard (Step 2 of 3)

Configure the ingest modules you would like to run on this data source.

- Recent Activity
- Hash Lookup
- File Type Identification
- Embedded File Extractor
- Exit Parser
- Keyword Search
- Envi ron Parser
- Extension Mismatch Detector
- EOL Verifier
- Android Analyzer
- Interesting Files Identifier
- PhotoRec Viewer
- Process Unallocated Space

Select keyword lists to enable during ingest:

- Phone Numbers
- Email Addresses
- IP Addresses

Scripts enabled for string extraction from unknown file type

- Latin - Basic
- Encodings: UTF8, UTF16

Performs file indexing and periodic search...
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?