

9th Annual

#OSDFCon

OPEN SOURCE DIGITAL FORENSICS CONFERENCE

Messaging App Forensics with Autopsy

Brian Carrier

October 17, 2018 | Herndon, VA | Hosted by



Motivation

Show users new features around messaging, email, and chats.

Show developers how to use the new infrastructure.

This work was all funded by DHS Science and Technology (S&T).

Main Autopsy UI

The screenshot displays the main interface of the Autopsy digital forensics software. The top menu bar includes options like 'Add Data Source', 'Images/Videos', 'Communications', 'Timeline', 'Generate Report', and 'Close Case'. On the left, a sidebar shows a tree view of data sources, with 'Extracted Content' expanded to show various file categories such as 'Devices Attached (3)', 'EXIF Metadata (9)', 'Installed Programs (23)', and 'Web Search (130)'. The main window is titled 'Listing' and shows 'EXIF Metadata' for 9 results. A table lists the source files with columns for 'Source File', 'S', 'C', 'O', 'Date Created', 'Device Model', and 'Device Make'. The file 'ACC93d01' is highlighted in blue. Below the table, a row of tabs includes 'Hex', 'Strings', 'Application', 'Indexed Text', 'Message', 'File Metadata', 'Results', 'Annotations', 'Other Occurrences', 'Windows Registry View', and 'Video Triage'. The 'Results' tab is active, displaying a thumbnail of a photograph of young girls in white dresses with yellow flower leis.

Source File	S	C	O	Date Created	Device Model	Device Make
Tony_normal[1].jpg				2009-08-15 19:15:56 EDT	Canon EOS DIGITAL REBEL X5	Canon
QUPANq5X_normal[1].jpg					Desire HD	HTC
ta_520n-tfb-tm[1].jpg				2009-08-25 18:22:50 EDT	KODAK EASYSHARE V1003 ZOOM DIGITAL CAMERA	EASTMAN KODAK COMPANY
ame_8vc-tfb-tm[1].jpg				2009-08-25 18:20:18 EDT	KODAK EASYSHARE V1003 ZOOM DIGITAL CAMERA	EASTMAN KODAK COMPANY
80137d01				2011-02-08 07:50:30 EST	NIKON D700	NIKON CORPORATION
ACC93d01				2007-07-21 10:48:42 EDT	Canon EOS-1D Mark III	Canon
F733Fd01				2006-03-30 12:34:35 EST	Canon EOS-1Ds Mark II	Canon

Email: The Old Way

The screenshot displays an email client interface. On the left is a navigation pane with folders like 'Keyword Hits', 'Hashset Hits', 'E-Mail Messages', and 'Default (259)'. The main area shows a list of messages, with the selected message being 'alex: alex@m57.biz' with subject 'FW: UFOs Over U.S.'. Below the list is a toolbar with tabs for 'Hex', 'Strings', 'Application', 'Indexed Text', 'Message', 'File Metadata', 'Results', 'Annotations', and 'Other Occurrences'. The 'Results' tab is active, showing 'Result: 6 of 1907'. The detailed view below shows the HTML source code of the message.

Type	Value
Message (HTML)	<pre><!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"> <HTML><HEAD><TITLE>CNN.com - Larry King</TITLE> <META http-equiv=Content-Type content="text/html; charset=us-ascii"> <STYLE type=text/css>.cnnMainBody { FONT-SIZE: 12px; FONT-FAMILY: verdana, "Lucida Sans Typewriter", helvetica } </STYLE> <META content="MSHTML 6.00.2900.5512" name=GENERATOR></HEAD></pre>

SMS: The Old Way

The screenshot displays a mobile forensics application interface. On the left is a navigation pane with categories like Data Sources, Views, Results, Keyword Hits, Hashset Hits, E-Mail Messages, Interesting Items, Accounts, Tags, and Reports. The 'Results' section is expanded to show 'Extracted Content' with sub-items: Call Logs (108), Contacts (12), EXIF Metadata (139), Encryption Suspected (1), Extension Mismatch Detected (632), GPS Route (9), GPS Trackpoints (1), and Messages (79). The 'Messages' category is selected.

The main window shows a 'Listing Messages' table with columns: Source File, S, C, O, Direction, From Phone Number, To Phone Number, and C. A grey box redacts the 'From Phone Number' and 'To Phone Number' columns for several rows. The selected row is highlighted in blue.

Source File	S	C	O	Direction	From Phone Number	To Phone Number	C
mmssms.db				Outgoing		70	2
mmssms.db				Incoming	+1		2
mmssms.db				Outgoing		70	2
mmssms.db				Incoming	+1		2
mmssms.db				Outgoing		70	2
mmssms.db				Outgoing		70	2

Below the table is a search bar showing 'Result: 48 of 60' and navigation arrows. A 'Results' tab is active, displaying a detailed view of the selected message:

Type	Value
Direction	Incoming
From Phone Num	+1 [redacted]
Date/Time	2013-09-13 20:49:48
Read	Read
Subject	
Text	I have other ideas in mind. She will hand it all to me!

Problem / Solution

Problem: Hard to sort through large amounts of messages

Why: Autopsy stores and displays things in generic ways so that it can support unknown data types. It's a general framework.

Solution: Store and display messages in more efficient ways.

What Questions Did We Focus On

Triage

- What are the most communicated with accounts?
- What kinds of media was this person sharing?
- What communication types was this person using?
- What were the most recent conversations?

Deep Dive:

- What is the social network for this device?
- What are the themes and topics in the messages?

Change #1: New Content Viewer

A new Message content viewer exists in the lower right. Shows:

- Headers
- Various formats of emails (HTML, RTF, etc.)
- Attachments
- Can load external images (if you opt-in)

New Content Viewer

The screenshot shows a web-based email viewer interface. At the top, there is a navigation bar with tabs: Hex, Strings, Application, Indexed Text, Message (selected), File Metadata, Results, Annotations, Other Occurrences, and Video T. Below the navigation bar, the email header is displayed in a grey background:

From: alex: alex@m57.biz
To: jean@m57.biz
CC:
Subject: FW: UFOs Over U.S. Military Sites?

Below the header, there is another set of tabs: Headers, Text, HTML (selected), RTF, and Attachments (0). The main content area shows a video player with a red 'x' icon in the top left corner. The video player displays the following text:

Larry King Live at 9:00pm ET
on Friday, July 18, 2008

Tonight: UFOs Over U.S. Military Sites?

Have UFOs disabled U.S. defense systems?
Wait until you hear what three

New Content Viewer (Attachments)



From: Microsoft Outlook 2000

To:

(It's hard to find public data...)

CC:

Subject: Welcome to Microsoft Outlook 2000!

Headers Text HTML RTF Attachments (8)

Table Thumbnail

Page: 1 of 1

Pages:



Go to Page:

Images: 1-8

Medium Thumbnails

Sort



wmt.gif



exchange.gif



ie.gif



yellowbg.gif

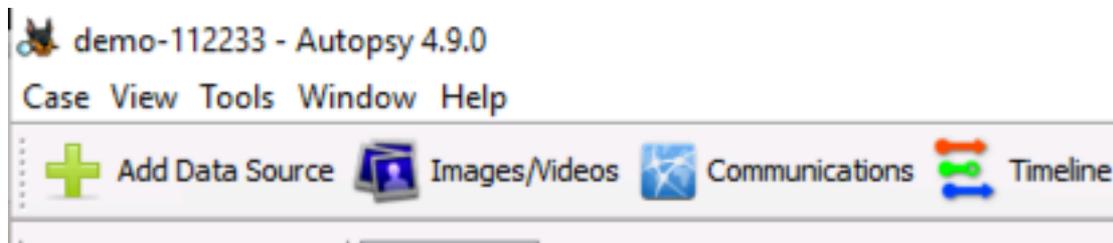


netmeeting.gif

Change #2: New UI

The generic tree interface in Autopsy does not easily answer the previous questions.

So, we made a new one.



New Communications UI

The screenshot displays a user interface for managing communications. It is divided into several sections:

- Filters:** Includes 'Apply' and 'Refresh' buttons.
- Devices:** A list of devices with checkboxes, including 'bk0_nmcbk0.bin' and 'outlook.dd'. 'Uncheck All' and 'Check All' buttons are present.
- Account Types:** A list of account types with checkboxes, including 'Device', 'Phone', 'Email', 'Facebook', 'Twitter', 'Instagram', 'Facebook', 'MessagingApp', and 'Mibelle'. 'Uncheck All' and 'Check All' buttons are present.
- Date Range:** A section for filtering by date range, currently set to 'America/New_York' with a start date of 'September 22, 2018' and an end date of 'October 13, 2018'.
- Message List:** A table with columns: Account, Device, Type, and Msgs. It lists various accounts and their associated message counts.
- Message Detail View:** A detailed view of a selected email from 'alex: alex@m57.biz' dated '2008-07-19 19:32:54 EDT'. The subject is 'FW: UFOs Over U.S. Military Sites?'. The body text includes: 'on Friday, July 18, 2008', 'Tonight: UFOs Over U.S. Military Sites?', and 'Have UFOs disabled U.S. defense systems?'. Below the text are tabs for 'Headers', 'Text', 'HTML', 'RTF', and 'Attachments (0)', along with a 'Show Images' button.

UI Basics: Filters

Reduce the scope of messages and accounts based on:

- Dates
- Account Types
- Devices

The screenshot displays a filter configuration interface with the following sections:

- Filters:** Includes 'Apply' and 'Refresh' buttons.
- Devices:** A list with two items: 'blk0_mmcbk0.bin' and 'outlook.dd', both checked. Below the list are 'Uncheck All' and 'Check All' buttons.
- Account Types:** A list with ten items: 'Device', 'Phone', 'Email', 'Facebook', 'Twitter', 'Instagram', 'Facebook', 'MessagingApp', and 'Mobile'. All items are checked. Below the list are 'Uncheck All' and 'Check All' buttons.
- Date Range (America/New_York):** Includes 'Start' and 'End' fields. The 'Start' field is set to 'September 22, 2018' and the 'End' field is set to 'October 13, 2018'. Both fields have a dropdown arrow to the right.

UI Basics: View Accounts



Accounts that meeting
filters are shown.

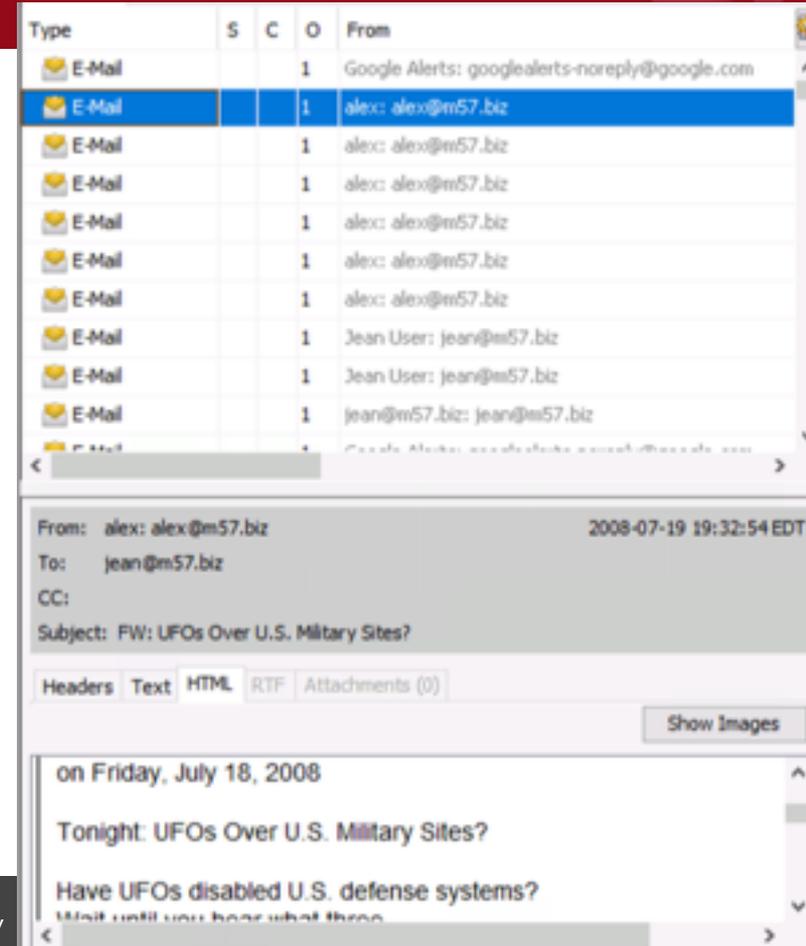
Sorted by number of
relationships.

Only accounts with a
relationship are shown
(not random emails)

UI Basics: View Messages

Shows all messages to/
from an account.

Bottom shows message
contents,
attachments, etc.



UI Basics: Link Analysis

Visualization of the data can be useful.

Link analysis diagrams can quickly become overwhelming.

We chose an “Opt-In” method:

- Right click on an account and choose “Add Selected Account to Visualization”.
- That shows the account and all associated with it.

UI Basics: Link Analysis

Selecting an Account

Account	Device	Type
 jean@m57.biz	outlook.dd	Email
 googlea		
 +		
 4:		
 newsletters@n.npr.org	outlook.dd	Email
 alison@m57.biz	outlook.dd	Email
 alex@m57.biz	outlook.dd	Email

Properties

-  Add Selected Account to Visualization
-  Visualize Only Selected Account

UI Basics: Link Analysis

The screenshot displays a link analysis tool interface. The central node is 'jean@m57.biz', which is connected to several other nodes, including 'alex@m57.biz', 'googlealerts-noreply@google.com', 'npr-accounts@npr.org', 'bob@m57.biz', 'allsonsg@n.npr.org', 'carol@m57.biz', 'accounts-noreply@google.com', 'admin@assistedcontent.com', 'newsletters@n.npr.org', and 'alison@m57.biz'. The interface includes a 'Filters' section with 'Apply' and 'Refresh' buttons, a 'Browse' and 'Visualize' section with 'Clear Viz.' and layout options ('Fast Organic', 'Organic', 'Hierarchical', 'Circle'), and a 'Zoom: 150%' control. On the left, there are sections for 'Devices' (listing 'blk0_rmcblk0.bin' and 'outlook.dd') and 'Account Types' (listing 'Device', 'Phone', 'Email', 'Facebook', 'Twitter', 'Instagram', 'Facebook', 'MessagingApp', and 'Website'). On the right, there is a '167 relationships' section with a table of messages and a 'Google Web Alert for: Domain name: www.zu3...' section.

Filters: Apply Refresh

Browse Visualize

Clear Viz. Layouts: **Fast Organic** Organic Hierarchical Circle Zoom: 150%

Devices:

- blk0_rmcblk0.bin
- outlook.dd

Uncheck All Check All

Account Types:

- Device
- Phone
- Email
- Facebook
- Twitter
- Instagram
- Facebook
- MessagingApp
- Website

167 relationships

Messages

Type	S	C	O
E-Mail			1

From: Google Alerts: googlealerts-n
To: jean@m57.biz
CC:
Subject: Google Alert - m57.biz

Headers Text HTML RTP Attach

Google Web Alert for: i

[Domain name: www.zu3...](#)
... www.ymj83m.us www.qsl
www.m57.biz www.lhczv4.ul

This as-it-happens Google Alert

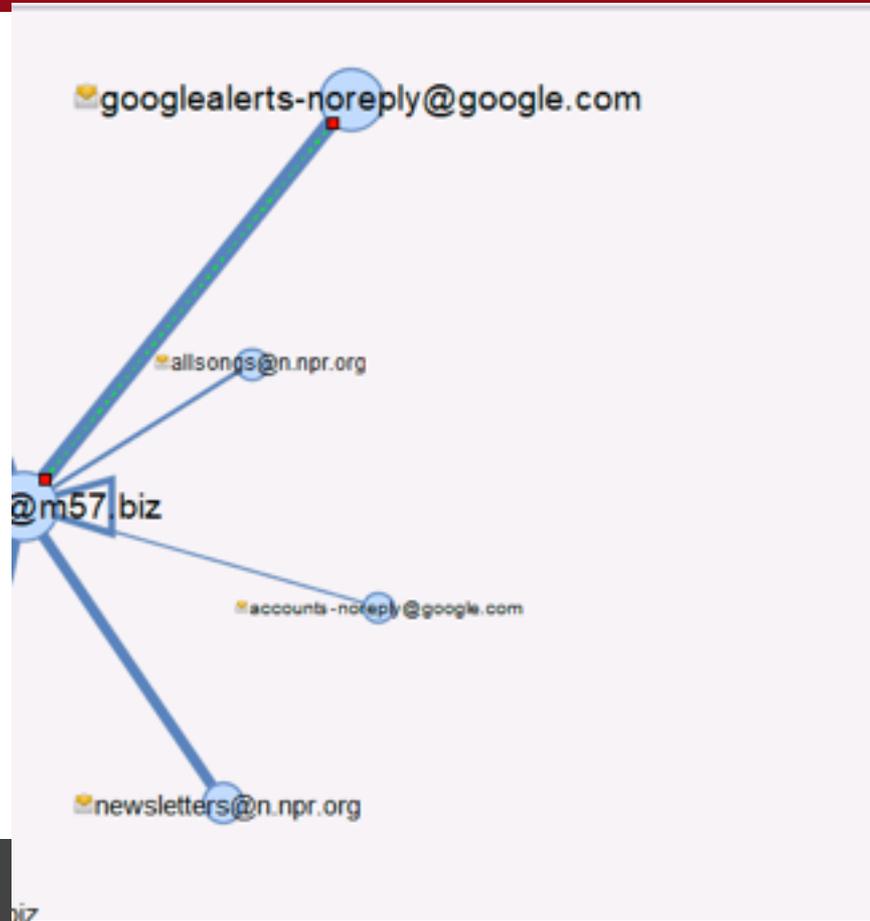
[Remove this alert](#)

UI Basics: Link Analysis

Selecting a node shows all messages to and from that account.

Selecting an edge shows messages between the two accounts.

UI Basics: Link Analysis



Type	S	C	O	From
E-Mail			1	Google Alerts: googleal
E-Mail			1	Google Alerts: googleal
E-Mail			1	Google Alerts: googleal
E-Mail			1	Google Alerts: googleal
E-Mail			1	Google Alerts: googleal
E-Mail			1	Google Alerts: googleal
E-Mail			1	Google Alerts: googleal

<

From: Google Alerts: googlealerts-noreply@google.com
To: jean@m57.biz
CC:
Subject: Google Alert - m57.biz

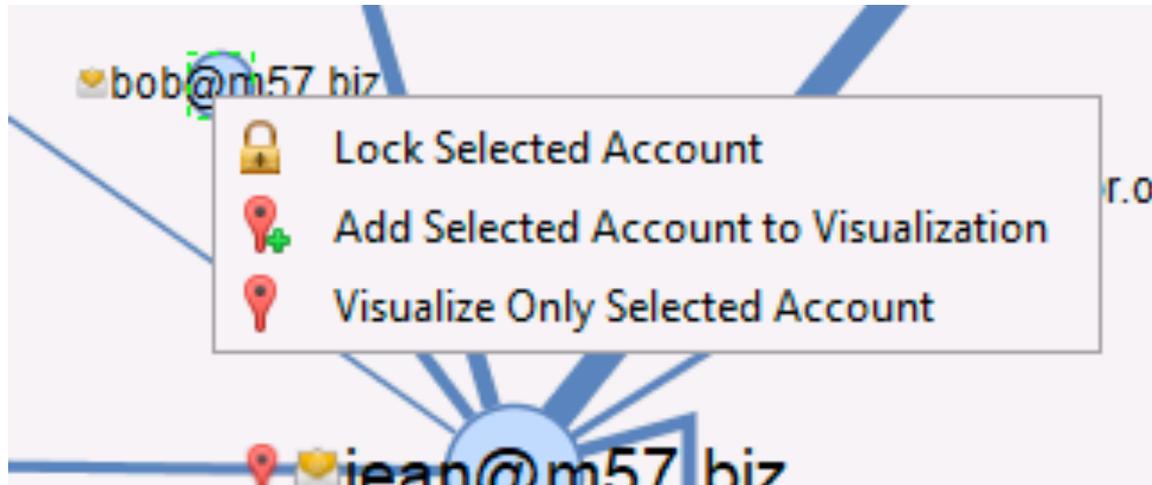
Headers Text HTML RTF Attachments (0)

Google Web Alert for: m57.biz

[Domain name: www.zu3.uk](#) [The Constellati](#)
... [www.ymj83m.us](#) [www.qsif.br](#) [www.dtnlh.net](#) w
[www.m57.biz](#) [www.ihczv4.uk](#) ...

Visualization: Adding More Accounts

Right click on an account to bring in all of its relationships:



Backend Framework

(Quick Overview For Developers)

Typical Scenario

You write a module to parse some kind of database to pull out messages.

You want to take advantage of this new UI.

Basic Approach

Create a Blackboard Artifact like you would for any other data type.

- Blackboard remains the primary place to store data from modules.

Add communications-specific data that points to the message artifacts.

Messages

Create a Blackboard Artifact

Example:

- Artifact Type: TSK_MESSAGE
- Attributes for recipients, content, headers, etc.

You can put whatever you have in here.

Accounts

Accounts have a type (such as email or Facebook) and an identifier (such as a@b.com)

You need to add an Account Instance for each file the account is found in.

```
senderAcct =  
CommManager.createAccountFileInstance(EMAIL,  
"a@b.com", sourceFile);
```

NOTE: exact syntax is slightly more verbose

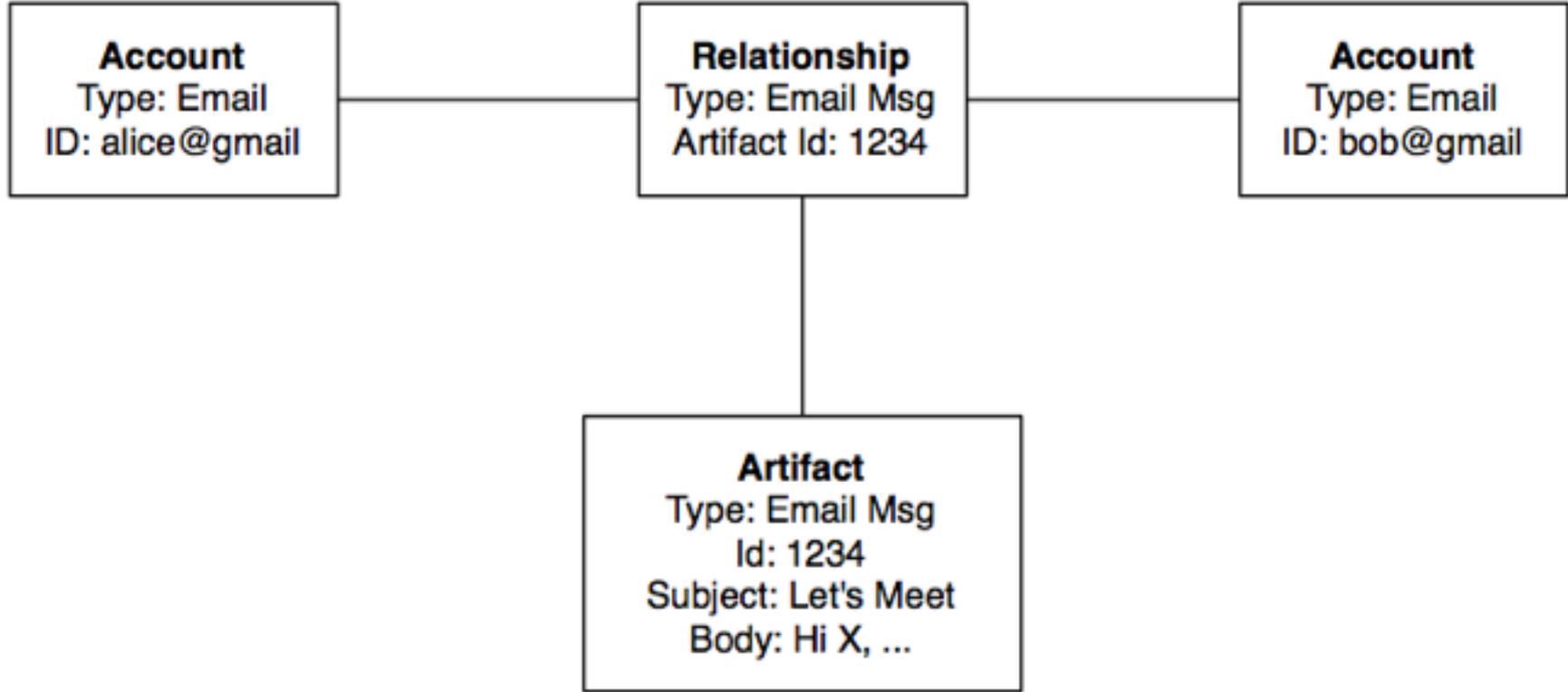
Relationships

A relationship occurs when two accounts “interacted” (i.e. sent message, made a call, in a contact book) at a given time.

Add to the database with:

```
CommMgr.addRelationship(senderAcct, List of receiverAccts,  
messageArtifact, TYPE.MESSAGE, “2018-10-17...”)
```

Visualization



Call To Action!

October 17, 2018 | Herndon, VA | Hosted by



We Need More Messaging Parsers

We built it, now we need more developers to come build parsers.

Build a Python parser for your favorite app.

Use the Android module or tutorials in Autopsy as a reference.

Next Steps

Roadmap

Scaling

Messages:

- Threading
- Thumbnails for attachments

Histogram for filtering

Automatically visualize the most communicated with accounts.

... LOOK AT

Questions?

brianc <at> basistech.com

Connect on LinkedIn

Provide future suggestions now,
during “Needs” session, or in survey.