

This quick reference for doing email analytics grew out of a webinar done by our partners Richard Wessel and Lindsay McGhee of NearZero Discovery. For more information, you may wish to consult our full [Guide to Advanced Email Analytics](#) or listen to the [recorded webinar](#).

Email Analysis 101



To begin, you must understand how the custodians managed their email. The following questions should be top of mind when interviewing custodians or reviewing someone's email data.

- Is the person a **PILER** or **FILER**?
- What type of documents were typically sent as **attachments**?
- Did the person actively use their **calendar**?
- What other mail features did they use? **Tasks**?
- What are the **date ranges** of the messages?
 - Are there any gaps in the email or calendar date ranges? If so, why?



Email Threading

The foundation of any good eDiscovery platform's email analytics lies in its email threading. Email threading is key to establishing the chain of communications and events to get a clear picture of which parties knew what details and when they knew them - telling the story of the case. Having a clear view into the email threads and how your system handles and exposes them is the core of any email analysis.

Uses:

- Establishing the chain of communications and meeting events
- Understanding who knew what and when
- Seeing who forwarded or responded to communications

Email Analysis Techniques

Step 1: Email Summary Reports

Email summary reports show the 10,000 foot view of your eDiscovery project at either the project, custodian or media level - email metrics, document and attachment counts, exclusion metrics for corrupt, password protected, or unsupported file types, and the date range included.

Utilize visualizations like VenioOne's Top 10 graphs to view the years encompassed, email addresses, and domains to rapidly determine how to proceed and what gaps there may be in the initial collection or processing of data.

Uses:

- Double check processing of data
- Meet and confer preparation
- Custodian interviews
- Internal investigations



Step 2: Domain Analysis

Domain analysis identifies relevant data and/or excludes irrelevant data in order to reduce the volume to be reviewed or produced. Excluding news, sports, advertising, and marketing emails can dramatically reduce the amount of data to be reviewed. Additionally, domain analysis can be very useful to locate emails to/from specific domains.

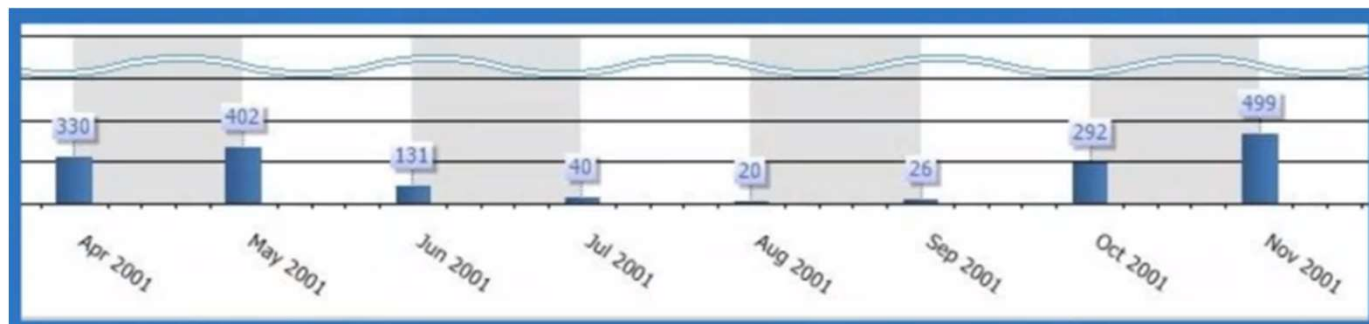
Uses:

- Employees leaving to work for a competitor
- Excluding irrelevant domains
- Identifying personal email to collect
- GDPR requests for deletion of personal data

Domain Types to Consider

- Old Domain Names
- News Websites
- Sports Websites
- Subscriptions
- Advertising/Marketing
- Junk/Spam
- Personal Email Domains, e.g. Yahoo, Gmail, AOL, Outlook.com

Step 3: Timeline and Gap Analysis



The more quick checks of data you can do in your early case assessments, the better. Being able to review a timeline and the volume of data for each day can be helpful for identifying where there may be gaps in data that was collected.

The ability to drill directly down into the timeline on known significant dates and then see all communications graphically can be much faster to do a quick review of important communications, especially when using threading or other visual diagrams to see relationships. Conversely, if you expect to see communications and there are none, then that may identify communications that have been deleted or excluded.

Uses:

- Confirming relevant data has been collected and processed
- Determining a custodian's role along the case timeline
- Filtering to relevant dates based on data

Step 4: Deleted Items Analysis

You must be familiar with how the email systems from which you are collecting handle deletions and what purge interval or soft deletion settings they may have to understand what may or may not be included in your collection. Beyond that, being able to answer the all important question of "Do we have everything?" is critical.

Uses:

- Identification of the smoking gun email that may have been deleted
- Demonstrating preservation of all documents after legal hold initiation
- Finding items that may be in Deleted Items or Trash folders prior to legal hold initiation

Advanced Email Analytics: Thinking Outside of the [IN]box

Step 5: Folder Analysis

Instead of running keyword searches, email folder analysis can more quickly narrow down which custodians may have relevant content and how much content exists. You can also gain insight for formulating keyword searches based on the terminology used by custodians to organize their communications.

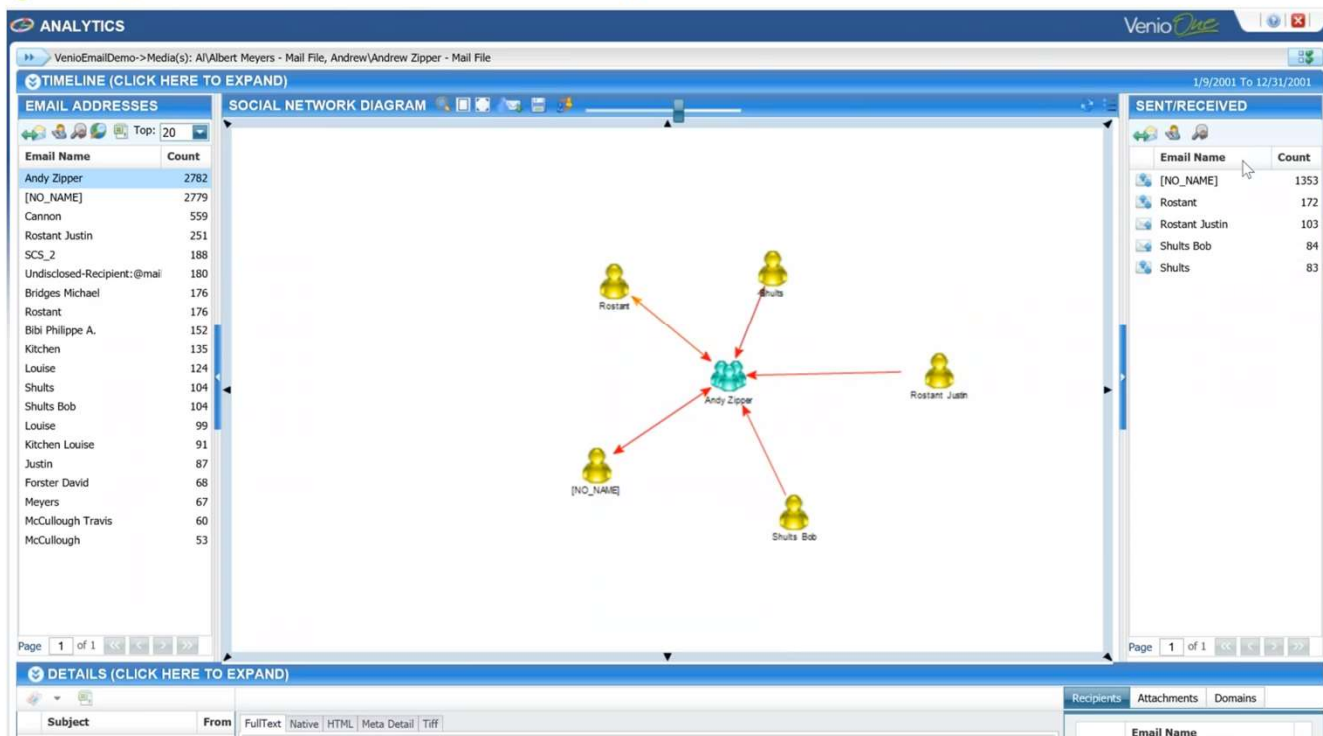
Folder analysis can be particularly helpful outside of litigation settings when internal audits are being done or for analyzing traffic from web filtering and monitoring tools.

Uses:

- Identifying relevant content by custodian and volume of content
- Gain insight into terminology used to formulate searches
- Internal Data Audits
- Analyzing web filtering/monitoring traffic

Folder Name	Document Count
System Folder	0
AI	0
Albert Meyers - Mail File	0
albert_meyers_000_1_1.pst	0
Personal folders	0
meyers-a	0
ExMerge - Meyers, Albert	0
Sent Items	14
Inbox	22
Deleted Items	1,131
Contacts	4

Step 6: Social Network Diagram



Advanced Email Analytics: Thinking Outside of the [IN]box

Newer features like VenioOne's Social Network Diagram bring to life the phrase "A picture is worth a thousand words" - relationships are clearly noted and the volume and direction of communication are clearly marked. Diagrams can be saved as images to assist during interviews with custodians and other parties or to visualize email evidence. Additionally, emails can be viewed and tagged from within the tool to save review time. Attached documents are even included with various options for viewing and downloading. Being able to effectively use these types of modern tools is like having eDiscovery super powers!

Uses:

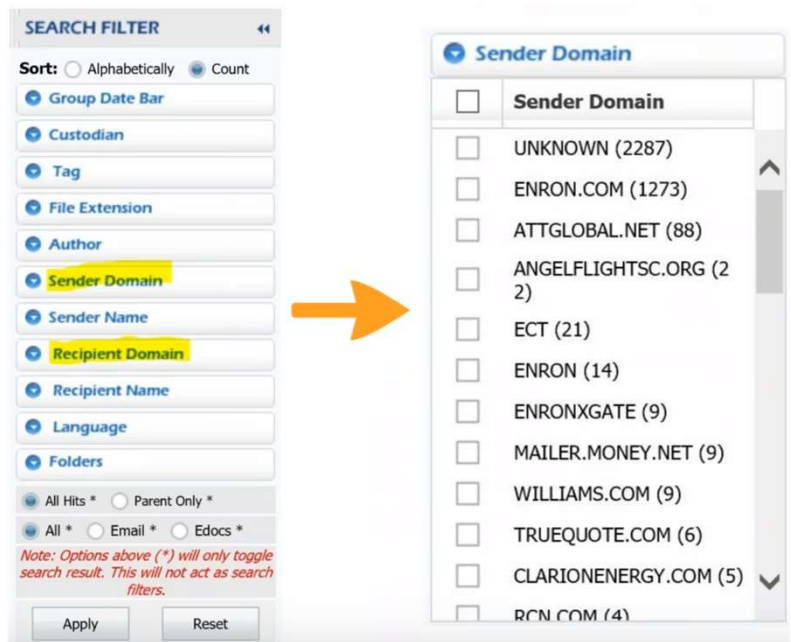
- Quickly digging into details without having to use search tools
- Seeing things you might not have expected
- Identifying custodians using multiple email accounts
- Visualizing communications for data privacy, security, and compliance initiatives

Combined Forces

Don't think of email analysis tools in isolation. All of the above can be used in combination with things like dynamic folders and searching to create powerful solutions. For example, filter searches by sender or recipient domain (as shown).

HOT TIP

Build a search to use across multiple projects that contains known sports or news sites. Use that search to populate a dynamic folder and easily tag any non-relevant items.



The screenshot shows the 'SEARCH FILTER' interface. On the left, a list of filters includes 'Sender Domain' and 'Recipient Domain', both highlighted in yellow. An orange arrow points from the 'SEARCH FILTER' panel to a 'Sender Domain' results panel on the right. This panel displays a list of domains with checkboxes and counts:

<input type="checkbox"/>	Sender Domain
<input type="checkbox"/>	UNKNOWN (2287)
<input type="checkbox"/>	ENRON.COM (1273)
<input type="checkbox"/>	ATTGLOBAL.NET (88)
<input type="checkbox"/>	ANGELFLIGHTSC.ORG (22)
<input type="checkbox"/>	ECT (21)
<input type="checkbox"/>	ENRON (14)
<input type="checkbox"/>	ENRONXGATE (9)
<input type="checkbox"/>	MAILER.MONEY.NET (9)
<input type="checkbox"/>	WILLIAMS.COM (9)
<input type="checkbox"/>	TRUEQUOTE.COM (6)
<input type="checkbox"/>	CLARIONENERGY.COM (5)
<input type="checkbox"/>	RCN.COM (4)

Uses:

- Covering your bases
- Filtering out known domain names
- Identifying viruses within content