



**DIGITS LLC**

# **Evidence Analyzer**

**Email Edition  
Quick Start Guide**

**This page intentionally left blank**



## **Welcome to Evidence Analyzer: Email Edition**

Thank you for your purchase of the Evidence Analyzer: Email Edition - the pre-eminent tool that represents the next generation of intensive data analysis.

Evidence Analyzer: Email Edition, is a stand-alone forensic-grade software package for Microsoft Windows and Apple Macintosh based computers running either 32 or 64 bit operating systems. It is designed to independently read and interpret the data contained in the most commonly used email formats used today on both the desktop as well as the server.

Evidence Analyzer: Email Edition takes the guesswork out of email data analysis. Leveraging the power of features such as full content access, “blind” date filtering, non-restrictive tagging, de-duplication based accepted criteria, and full text indexing of message content and most common types of attachments it puts tremendous processing power in a small package. All of this is combined into a unified user interface that works along with the workflow of the user, rather than as a separate tool to be specifically learned. If a user is familiar with an email client such as Microsoft Outlook, Mozilla Thunderbird, or even Apple Mail; Evidence Analyzer: Email Edition will feel natural and familiar. Power and simplicity are the keywords. Evidence Analyzer: Email Edition is a tool that molds itself around how you want to work rather than forcing you to adapt.

Evidence Analyzer: Email Edition has combined a cutting edge user interface with the features most demanded by high volume professionals. Many features are packed into a small package.



## I. Introduction

Evidence Analyzer: Email Edition is a stand-alone software package for Microsoft Windows and Apple Macintosh based computers running either 32 or 64 bit operating systems. It is designed to independently read and interpret the data contained in the most commonly used email formats used today on both the desktop as well as the server.

Evidence Analyzer: Email Edition takes the guesswork out of email data analysis. Leveraging the power of features such as full content access, “blind” date filtering, non-restrictive tagging, de-duplication based on common data with user definable confidence levels, and full text indexing of message content and most common types of attachments. All of this is combined into a unified user interface that works along with the work-flow of the user rather than as a separate tool to be specifically learned. If a user is familiar with an email client such as Microsoft Outlook, Mozilla Thunderbird, or even Apple Mail; Evidence Analyzer: Email Edition will feel natural and familiar.



## II. System Requirements

The minimum system requirements for Evidence Analyzer: Email Edition are:

- A computer running a modern version of Microsoft Windows Vista or later or Apple Macintosh OSX 10.6 or later,
- A multi-core processor,
- At least 2GB of Random Access Memory,
- Enough free hard drive space to hold source files as well as resulting container files.
  - Use the formula: Original Data \* 3 = recommended free space
- Java virtual machine appropriate for your operating system and architecture
  - **NOTE: Ensure your versions match for 32bit or 64bit!**

The recommended system requirements are:

- All of the above except,
- At least 8GB of random access memory.

The processing and indexing portions of Evidence Analyzer: Email Edition is very memory intensive. The more RAM that is available for the system the better. Once the data is processed however, the memory is freed and the application itself has a rather small footprint. Once processed, case files can easily be accessed by lesser machines at or possibly even below the recommended minimums.



### III. Capabilities

Evidence Analyzer: Email Edition can process and allow the review of email data stored in the following formats:

- Microsoft Outlook PST (ANSI format used prior to Outlook 2003)
- Microsoft Outlook PST (Unicode Format used from Outlook 2003 to current)
- Microsoft Outlook OST (Both Exchange Server-based and Hotmail-based)
- RFC-compliant Mail Files (Commonly known as EML format)
  - Individually or in groups
- RFC-compliant MBOX format
- MailDir format
  - Mail Spool structured
  - Server-based store
  - Courier-Imap style

For “Filesystem-as-a-file” formats, such as Microsoft PST and OST files, Evidence Analyzer has additional capabilities for recovering deleted email as well as email that has been moved to trash and then deleted from trash (aka Deleted-Deleted). This is a method that relies highly on the overall condition and state of the container as well as the normal usage patterns and external system settings and behaviors. Results are in no way guaranteed as to the completeness of recovered data or even if data can be recovered at all. This can be a very useful feature, but as with any recovered semi-structured data residing in unallocated space, care should be taken when drawing conclusions based solely on it.

#### Indexing

Evidence Analyzer: Email Edition has a full text indexing capability that will allow searching through all properties, headers, and content sections of source data. Many of the most commonly used files and formats are also parsed and the textual content indexed where appropriate. A partial listing of compatible files follows below:

- Plain Text
- HTML
- XML and derivative formats
- Microsoft Office Documents (Content and Metadata)
  - OLE Based compound document types (pre-Office 2007)
  - OOXML Format (post-Office 2007)
- Open Document Format (ODF)
  - OpenOffice Formats
  - Other ODF-based Office and Productivity Suites
- Portable Document Format (PDF)



- Text Extractable PDF
- Metadata
- Cannot index pure image content (non-OCR scanned documents)
- EPUB Format used on many ebooks and other types of documents
- Rich Text Format
- Compressed Documents (of supported types)
- Java Class Files
- Audio, Video, and Image Metadata

Indexing for searching is a **VERY** resource intensive process and can take considerable time depending on the general makeup of the source container. Email containers without any attachments take the least amount of time to index. Adding indexing along with attempting to recover deleted fragments will take longer. Source files containing many attachments or attachments of large sizes will take much longer. **MUCH OF THIS TIME CAN BE MITIGATED THROUGH THE USE OF MORE RAM, FASTER HARD DISKS, OR OTHER MEANS.** On average, you can expect, on a system with the recommended specifications, 100MBs processed per 90 seconds. A 1GB container will take, on average, approximately 15 minutes to process and index.

### “Blind” Filtering

Evidence Analyzer: Email Edition allows for date-based restrictions. This allows a user to zero-in on a specific range of dates for examination. If known, this provides a fast and efficient means to limit the number of items to be reviewed and can substantially decrease review time. Date restriction is a pre-process selection, therefore the only content being processed into Evidence Analyzer: Email Edition will be items matching the selected criteria. This makes for the perfect option when the reviewer is legally or otherwise required to only look at specific items based on date.

Unlike some other products on the market, Evidence Analyzer: Email Edition is designed to attempt to evaluate the “best” date rather than the “easiest” date. Evidence Analyzer: Email Edition is a product designed by experienced Internet investigators and network administrators, which means that we know email and the finer points of finding the truth it contains. Simply using a date in the header of a message is not always enough. We evaluate all the dates available, which means in the case of PST and OST files, we also evaluate the metadata and properties file attributes to determine if the date recorded in the email header is true and accurate. The most logical date is used for filtering through evaluation by our proprietary logic algorithms.

### De-duplication

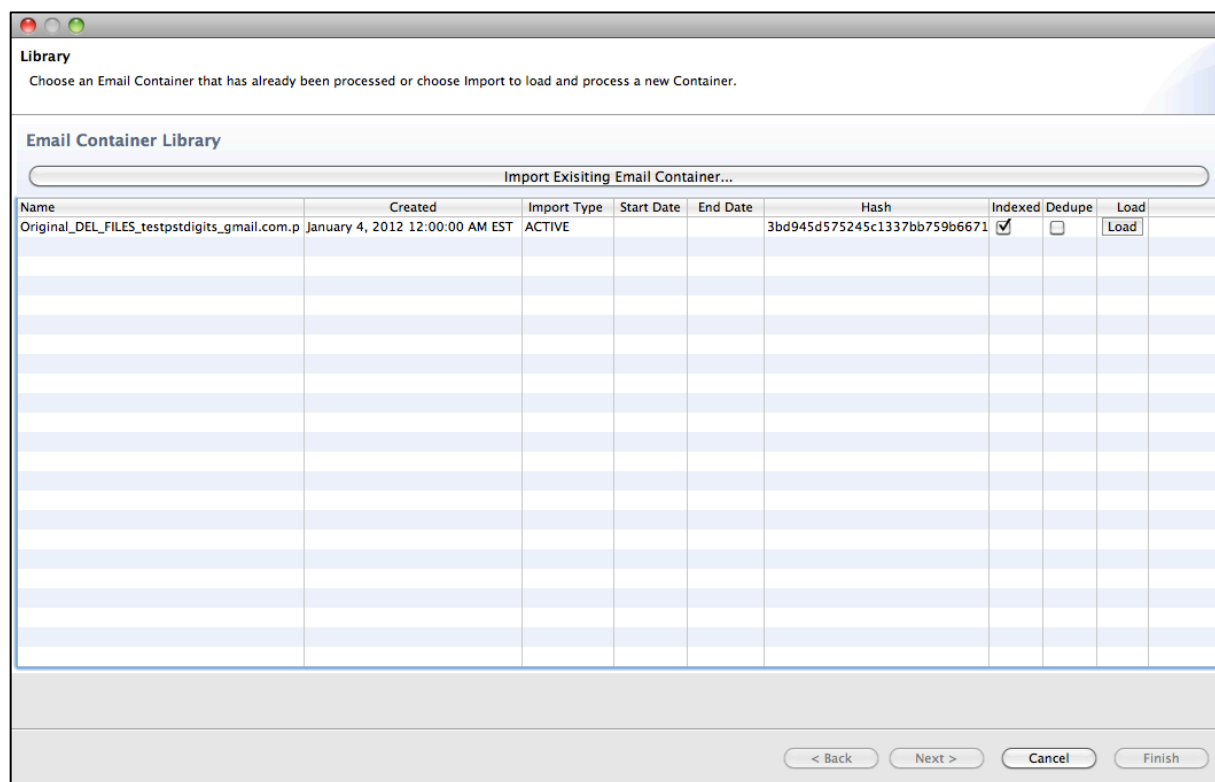
Evidence Analyzer: Email Edition allows for in-container de-duplication. This process uses an algorithm based on industry-standards that evaluates several headers and content to create a unique key that can be evaluated against.



## IV. Process

The Evidence Analyzer: Email Edition process is deceptively simple – by design. Many tools require a lot of specialized knowledge, training, or just a lot of experience to truly be effective as a user. As Evidence Analyzer: Email Edition was designed; the first priority was simplicity and capability. How can this tool be as powerful as it needs to be and is expected to be while remaining simple enough for the common user to be effective? Through process flow – that’s how.

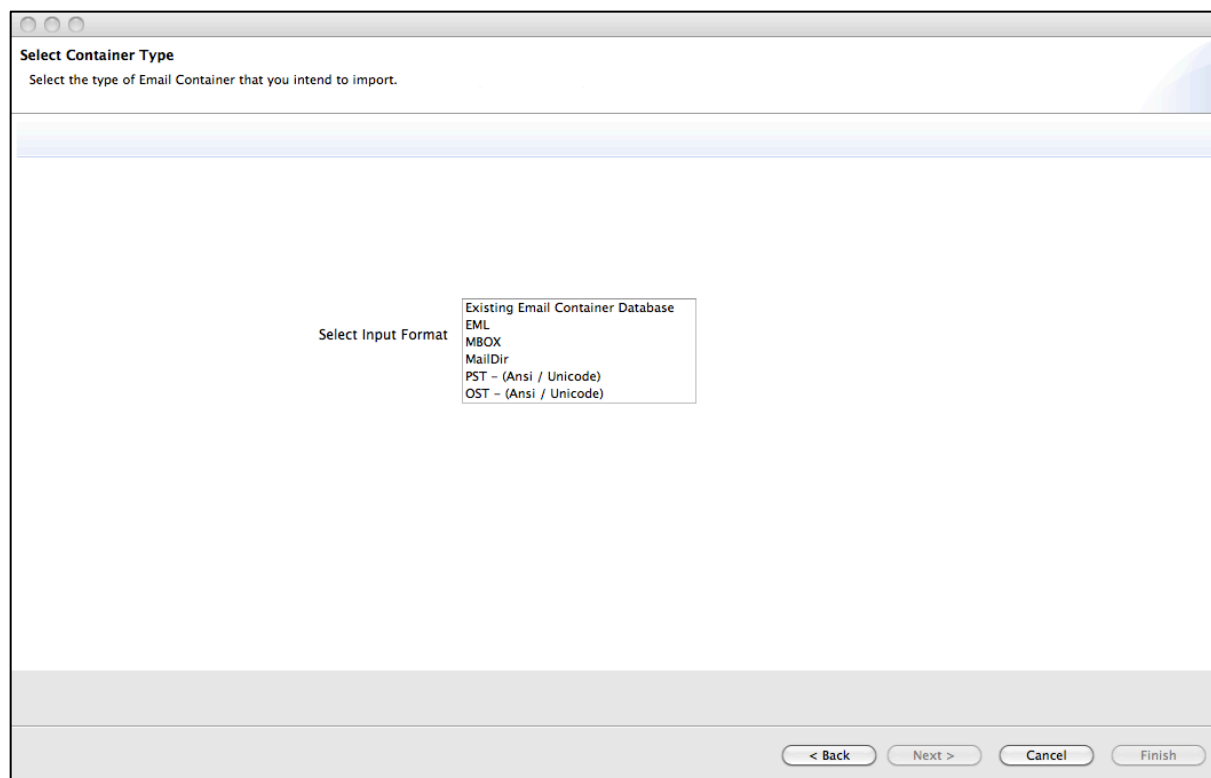
Evidence Analyzer: Email Edition is very simple to use. It’s even simple to set up to work with.



*Figure 1 – The Library View showing processed containers.*



When you decide to open an email container for processing and review, you will be presented with an inventory screen of all the cases you have processed along with the options they were processed with. You can choose to either load an existing container or a brand new container.



**Figure 2** – The Container Import Type selection screen.

Start with one of the supported container types. Simple types are simple to set up.

If you are working with one of the following:

- RFC-compliant email file or collection of files
- MBOX
- MailDir

You are working with a simple type. The data is only as it's presented, which means there is no option for recovering deleted items. You will be presented with choices during processing of date filtering and indexing. Indexing proceeds as normal and will work on all supported types. However, date filtering will rely on the data available within the header of each message due to the lack of any external metadata that could be used to corroborate the dates. You will also be asked to pick a location for data output. Simple and intuitive.



*Figure 3 – The MBOX Type import screen.*

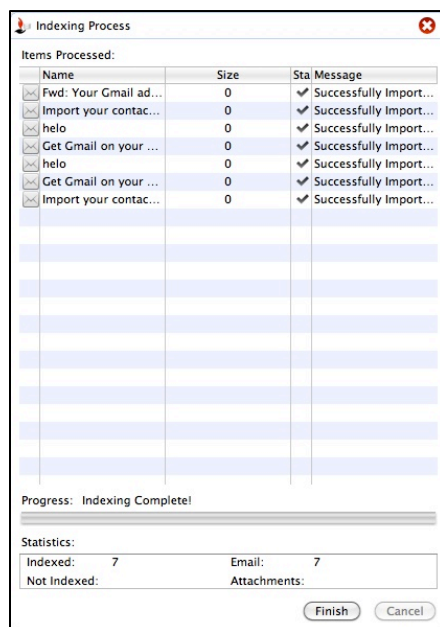
All file access is done in a read-only method. **NO SOURCE FILE WILL BE CHANGED OR MODIFIED DURING THE PROCESS.** Evidence Analyzer: Email Edition has been designed and validated to the highest standards of forensic evidence preservation.

Once everything is setup, you will be presented with a dialog to let you know how things are moving along. Roughly, the dialogs mean the following:

- 0% - 33%: The source file is being read,
- 34% - 66%: The items are being loaded into the program memory.
- 67% - 98%: The case file is built
- 99% - 100%: The user interface is created from the case file.



When Indexing is selected, a second dialog will be displayed:



*Figure 5 – The Indexing Status screen.*

- This window provides a rolling inventory of items seen and processed by the system.
- During this phase, the program can be used, but may be sluggish due to system usage and memory load. Unless absolutely necessary, it's recommended that the process be allowed to finish completely prior to using the program.

Once everything is complete, the user interface will be displayed. Items can then be browsed or searched.



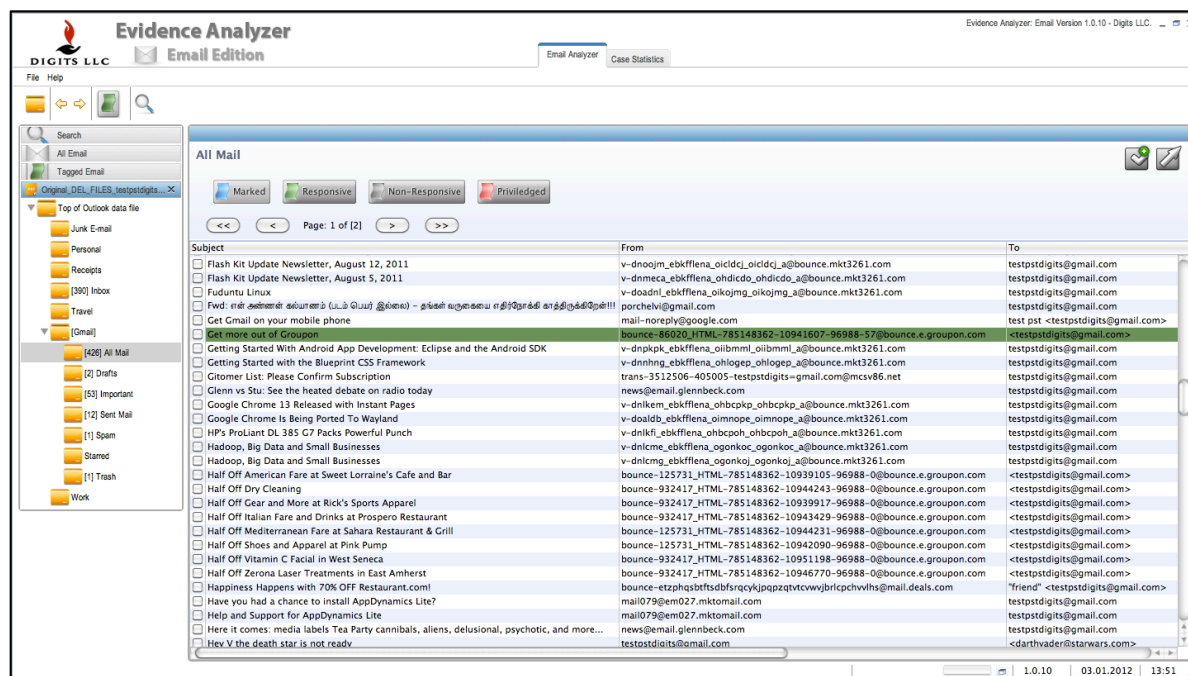


Figure 6 – The Main View screen.

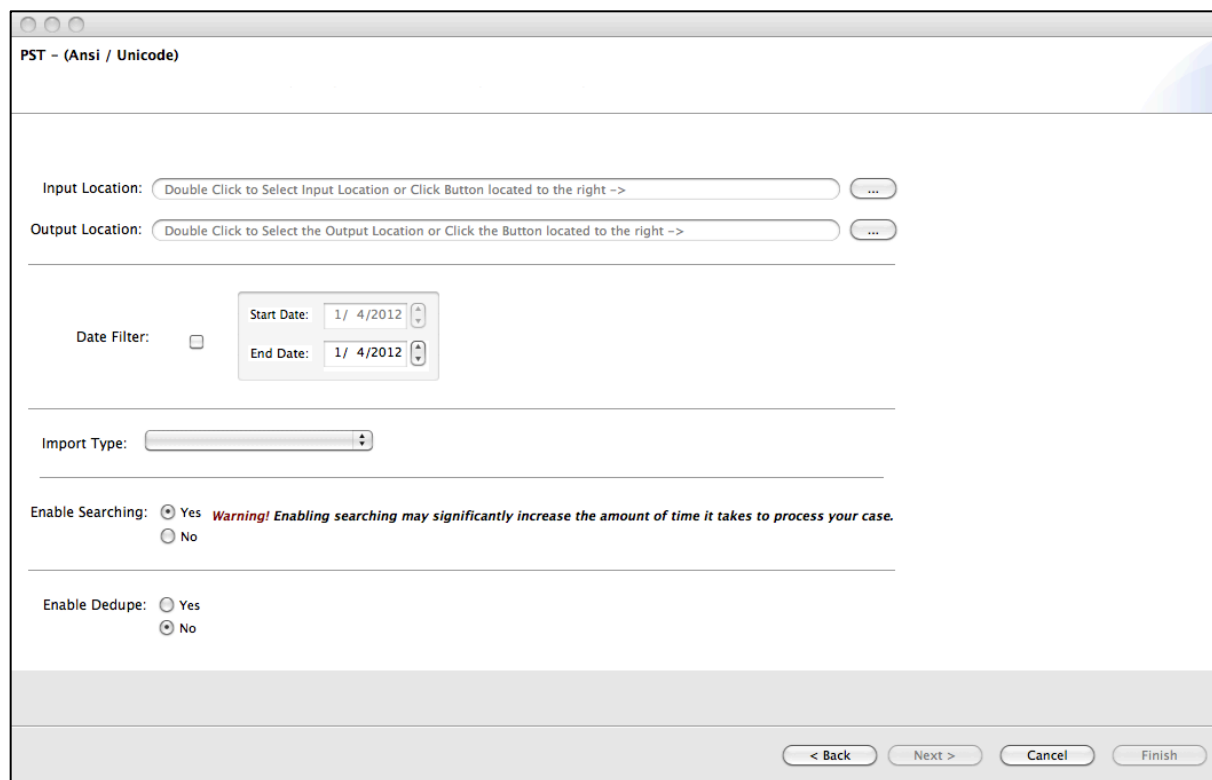
Non-simple file types are still pretty simple to set up. Just like for the basic types, you will be presented with the same options, but when you are accessing a PST or OST file, you will be presented with the additional options of obtaining just the Active Items, just the Recovered Items, or Both Active and Recovered.

Active email is the simplest option and will recover everything that would be displayed to a user using a native viewer.

Recovered only reads through all of the unallocated areas of the PST or OST container using our proprietary algorithm and attempts to recover data that used to exist as an active item.

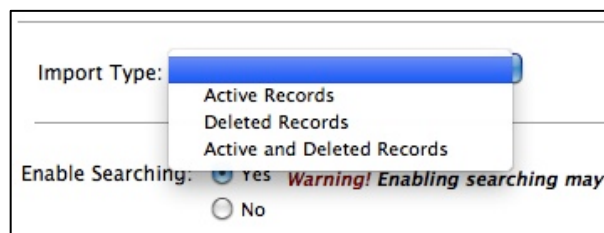
Selecting both will run both processes and display them both as distinct trees in the user interface.





**Figure 4** – The PST File type import screen.

The Recover option of PST / OST file processing is useful as well for extracting the data from a badly corrupted container or even a portion of a container.



**Figure 7** – Import Type Selection for PST / OST types

The dialogs and status bars presented during processing are the same for more complex types as simple types. Use them as a guide to gauge progress.



## V. Exporting Data

Evidence Analyzer: Email Edition allows two methods of data export. The first method is used when an entire case must be backed up or moved. This simply entails copying the created case files in the case folder. Everything is self contained and compartmentalized for simplicity.

EAAE is not a program that formally installs itself into the operating system. It runs as an executable of the Java Virtual Machine, but this does not create any specific system entries by way of Library entries on OSX or registry entries on Windows. Aside from the program files, case data is stored, by default, in a directory called “EAAE-Exports” that is located at the root of the running user’s home directory. All case and data files are stored here and can be copied or moved for archiving or backup purposes.

Second, you can export individual items. Each item will be exported to a place of your choosing defaulting to the “export” path location you chose at case setup. The item will be named according to the MD5 hash of the item as it is being written to disk. Email items will be written in RFC complaint format or easy importing into other tools or archiving. You can choose to preserve the directory hierarchy or flatten the files into one directory as you export.

Finally, multiple items exported in a batch will be written as an RFC-compliant MBOX to a location and with a name of your choosing.



## VI. Tagging

Tagging is a means to identify items of interest. A tag can be any word or phrase that allows the reviewer to identify or group the item at a later time. Tags tend to be more flexible and descriptive than a simple bookmark as well as simpler to set up and use.

Along with the free form tagging capabilities, Evidence Analyzer: Email Edition has four predefined tags set up that accommodate the normal functions of email style review. These tags are:

- “Responsive”,
- “Non-Responsive”,
- “Privileged”, and
- “Marked”.

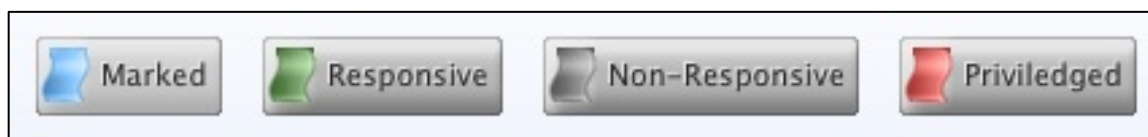


Figure 8 – Default Tags

Along with the tags, items marked with one of these tags are also color coded in all lists and views to allow for easy visual recognition. Responsive items are colored green; Non-responsive items are colored gray; Privileged items are colored red; and Marked items are colored blue.

This scheme allows a user to simply scan through a list of messages and know which have been reviewed and which have not. One more time saving measure.

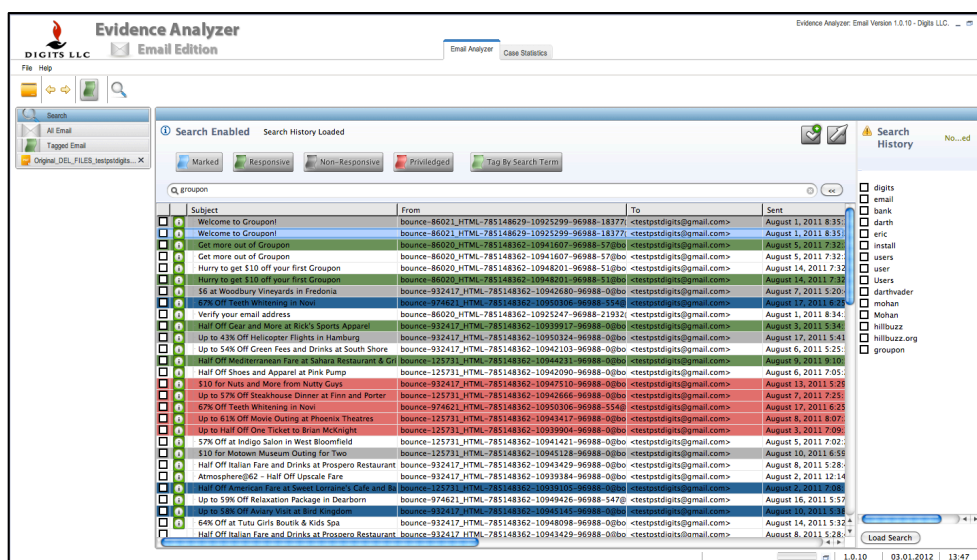


Figure 9 – Search View showing default tagged items



All tags are placed into a separate view that can be organized and even exported directly according to their groupings.

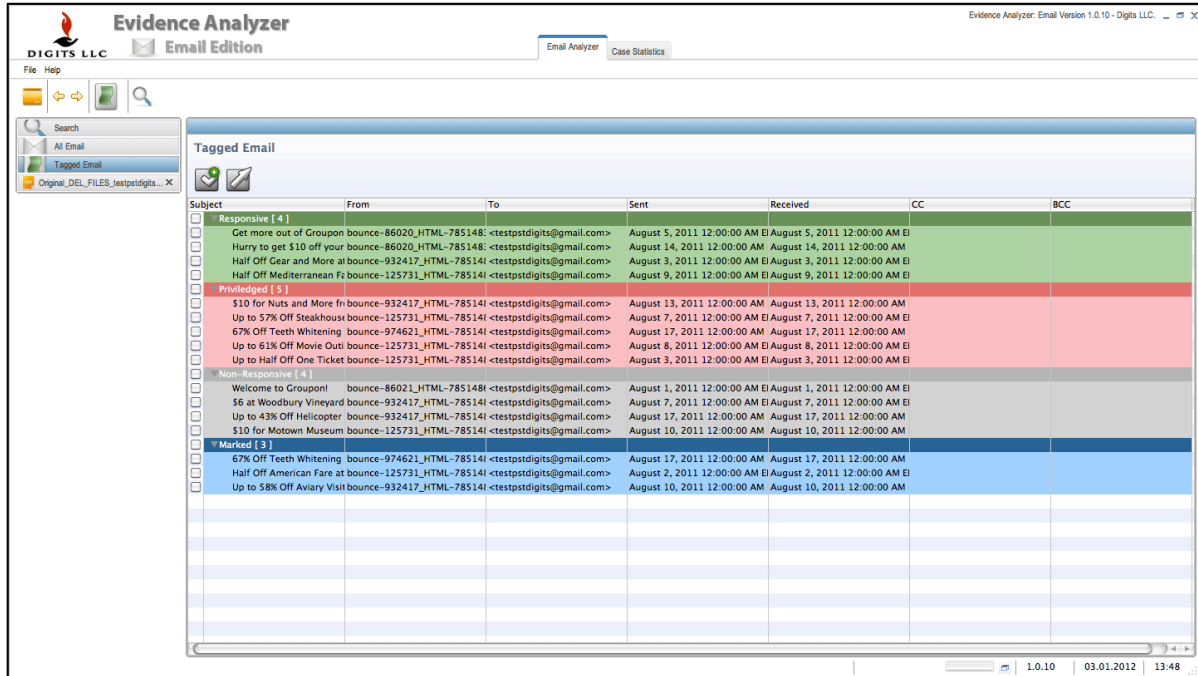


Figure 10 – Tagged items aggregated in the Tag View



## VII. Searching

Searching is enabled during case processing by enabling the indexing option. Indexing will take an input file and extract out all of the readable text and create a searchable index based on it. Indexing allows for almost instant search results to be displayed in the application, unfortunately, this is at the expense of up-front processing time. Indexing can take a lot of time depending on the input file, but sometimes the results are worth it.

Indexing is worth the expense in time if there is going to be extensive use made of keywords or if the source file is too large to do a sequential scan of all items.

Once an input file is processed and a case created, the data can be easily searched using the search bar. This bar appears on all views and can accept multiple types of input and syntax. Although keywords are commonly entered individually, much more can be done using the search bar.

The search bar supports queries using plain keywords, wild cards, fuzzy search, proximity search, Boolean operators, And, OR, as well as grouping. The search bar is VERY powerful.

- **Keyword:** “fraud” – would find all instances of the word “fraud”
- **Wild Cards:**
  - \* - “fraud\*” – would find all instances of “fraud”, “frauds”, or even “fraudster”
  - ? - “fraud?” – would only find a single character like “frauds” or “fraudz”
- **Proximity Search:** Append a tilde “~” to the end of a phrase along with an integer specifying distance
  - “Evidence Edition”~5 would find “Evidence Analyzer: Email Edition”
- **Boolean And / OR**
  - Placing “and” between keywords searches for an occurrence of both terms in a document
  - Placing “or” between keywords searches for an occurrence of either term in a document. This is the default operator when no others are specified and terms are not grouped.
- **NOT**
  - Negates whatever follows in search criteria
- **Grouping**
  - Parenthesis “()” can be used to group terms and operators
  - (black and white) or (blue or gray)



## VIII. Support Information

Support is offered to registered users of Evidence Analyzer: Email Edition.  
Register your copy today at <http://www.digitllc.com>

For support inquiries, please send your request to:

**[support@digitllc.com](mailto:support@digitllc.com)**

Please be as descriptive as possible in your request so we may better respond to your inquiry.



490 CENTER ROAD  
WEST SENECA, NY 14224  
T: 877-216-2511 F: 716-408-5549  
[www.digitllc.com](http://www.digitllc.com)

