

SUMMATION®
LEGAL TECHNOLOGIES, INC.

eDiscovery Workflow

White Paper

Published: July 2003

Updated: May 2004

For the latest information, please see <http://www.summation.com/papers/>

Abstract

This white paper is intended to provide an overview of Summation's eDiscovery Tools and provide a workflow model for managing electronic discovery (eDiscovery). The model emulates a legal scenario and shows how to use Summation to process, load, review, and produce eDiscovery. This document is also a valuable tool in orienting you with the procedures of electronic discovery.

© 2004 Summation Legal Technologies, Inc. All rights reserved.

The information contained in this document represents the current view of Summation Legal Technologies on the issues discussed as of the date of publication. Because Summation must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Summation, and Summation cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. SUMMATION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) or for any purpose, without the express written permission of Summation Legal Technologies, Inc.

Summation may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Summation, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

iBlaze and Summation Blaze are registered trademarks of Summation Legal Technologies, Inc. in the United States and/or other countries.

Microsoft is a registered trademark of Microsoft Corporation in the United States and/or other countries. Adobe and Acrobat are registered trademarks, and Distillers is a trademark, of Adobe Systems Incorporated. Lotus Notes is a registered trademark of International Business Machines Corporation. WordPerfect is a registered trademark of Corel Corporation.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Summation Legal Technologies, Inc. • 550 California Street • Sacramento Tower, 8th Floor • San Francisco, CA 94104 • USA



Contents

Introduction.....	1
Styles Used in This Document	1
Workflow Scenario.....	1
Processing eDiscovery	3
Processing an Entire Volume	3
Loading eDiscovery	8
Reasons to Load eDiscovery with the Built-in Summation Utilities.....	8
Loading Microsoft Outlook E-mail Messages and E-mail Attachments.....	8
Loading Electronic Document Files	14
Batch Loading eDiscovery Processed by a Service Bureau or Forensic Experts	17
Searching and Reviewing eDiscovery.....	21
Producing eDiscovery	25
Using Summation to Produce eDiscovery	25
Creating a Production Briefcase (Summation iBlaze edition only).....	29
Creating a Production Browser Briefcase (Summation iBlaze edition only).....	32
Using a Service Bureau to Produce eDiscovery.....	33
Appendices	34
Appendix 1: Glossary of Terms	35
Appendix 2: Electronic File Formats Supported by Summation’s Native Indexer	38
Appendix 3: The eDiscovery Console	39
Processing Selected .PST or .NSF Files.....	39
Using the View or Modify Mail Files Tab.....	40
Appendix 4: eDiscovery/Service Bureau Fields	42
Appendix 5: DII Tokens for Loading Electronic Documents or E-mail Messages	44
Appendix 6: Producing eDiscovery as Petrified Images	53
Petrifying eDiscovery	54
Producing eDiscovery from Petrified Documents.....	54
Appendix 7: Producing Compound Documents in Summation	56
The Burden of Production	56
Electronic Documents in Summation	56
Understanding Compound Documents	57
Producing Compound Documents.....	58
Privileged and Protected Documents	58



Petrification and Image Redaction	58
Appendix 8: Producing E-mail as a .PST File	59
Appendix 9: Using Electronic Evidence in the Deposition Process	60
Defining an Electronic Exhibit	60
Comparing Image File Formats to Native File Formats for Deposition Exhibits.....	61
Native File Format Benefits: The Availability of Metadata.....	61
TIFF and PDF File Benefits	62
Scenarios for Using Electronic Exhibits at Depositions	62
Displaying Electronic Exhibits	65
Using Summation for Handling Electronic Exhibits	65



Introduction

This white paper steps you through the processing of electronic discovery (eDiscovery, which includes electronic documents, e-mail messages, and e-mail attachments), loading electronic discovery into the Summation Blaze LG/iBlaze system, and preparing eDiscovery for production. Although the primary purpose of this white paper is to familiarize you with Summation's eDiscovery functionality, you can also use this white paper as a practical guide for the process of carrying out eDiscovery.

This white paper uses the Summation demonstration case *P. Franc v. K. Morris* to simulate a scenario and relate the functionality to your legal practice.

Note: *The Summation Blaze LG Gold and iBlaze editions of the Summation Blaze LG product line are the only editions that support eDiscovery handling.*

Styles Used in This Document

This white paper provides a number of visual cues to help guide you. The following styles are used in this document:

Italicized Text – Italicized text indicates a term that is specific to eDiscovery or to Summation. The first time a new term is used, it is italicized and accompanied by a definition, if needed. In addition, you can find all italicized terms in the *Glossary of Terms* appendix of this document.

Italicized text also indicates the title of another document or section within this document.

Bold Text – Bold text indicates an item that is found on the Blaze LG Gold or iBlaze interface, such as a menu option, a window, a field, or a dialog box.

`Courier New Font` – Text styled in Courier New font indicates text that you should type as a user.

Note: *Notes call attention to supplemental yet important information about the topics covered in this document. Notes also provide suggestions on how to deal more effectively with electronic discovery. Some of suggestions focus on Summation's tools while others have a broader scope.*

Workflow Scenario

The scenario outlined in this document is based on the Summation demonstration case *P. Franc v. K. Morris*, which is about a construction project gone awry. In this scenario, the client's electronic documents include e-mail messages, Microsoft Word® files, and Microsoft Excel® files, among other electronic formats. (For a complete list of electronic formats supported by Summation, refer to the *Electronic File Formats Supported by Summation's Native Indexer* appendix to this white paper.)

Note: *The scenario described in this document covers a portion of the electronic document formats supported by Summation. You can find information about loading other formats in the Batch Loading eDiscovery Processed by Service Bureau or Forensic Experts section of this white paper.*



The client's IT department has provided you with *volumes* (CD-ROMs, DVDs, hard drives, or other media used to store electronic documents) containing e-mail messages from key players' e-mail boxes bundled as Personal Folder Files (Microsoft Outlook archive files with the .PST file name extension), Microsoft Excel spreadsheet files, and Microsoft Word word processing files relating to the construction project at issue.

Note: *Although this scenario includes e-mail messages in .PST format only, the Summation **eDiscovery Console** supports e-mail messages in .NSF format (Lotus Notes format) and .MSG format (Microsoft Outlook message format).*

In this scenario, you will process and load the electronic discovery contained in the volumes provided by the client's IT department into Summation, before reviewing the documents. These volumes are referred to as *authenticating volumes*. (*Authenticating volume* is a term coined by Summation that refers to media obtained from a client or opposing party and contains electronic discovery in native file formats.)

During the course of the litigation, you received a request for production of documents by the opposing party. The opposing party is requesting all documents that mention or refer to the words "flood" or "flat space." The opposing party wants paper documents, e-mail messages in electronic format, e-mail attachments in their native formats, and electronic documents in their native formats.

This white paper explains how to complete all of these tasks.



Processing eDiscovery

This section explains the first step in using Summation to handle electronic information gathered during discovery: processing eDiscovery. Summation Version 2.5 and later includes a tool called the **eDiscovery Console** for processing.

During this stage, you will complete the following tasks:

- Move the electronic files that you received from your client or the opposing party into an existing case within Summation using Summation's **eDiscovery Console**. These files are located on some form of *storage medium* (such as a CD, a hard drive, and so on).
- Associate identifying information with the files and record comments relevant to them.

At the same time, the Summation **eDiscovery Console** will do the following:

- Provide you with a working copy of the files, which you can integrate for other uses in Summation.
- Offer you the ability to process the entire contents of the storage medium or, if you prefer, only a portion of the contents.
- Give you the opportunity to use a central location to manage electronic files gathered during discovery.
- Create a **Volume** folder with three other folders in it (the **PSTFiles** folder, the **NSFFiles** folder, and an **eDocFiles** folder) and separate e-mail files (.PST files from Microsoft Outlook and .NSF files from Lotus Notes) from individual electronic document files (such as a Microsoft Excel spreadsheet file) to simplify future loading.

Note: *If you choose to use a service bureau to batch load eDiscovery with Digital Image Information (DII) files, ask the service bureau to deliver two CDs to you: one with the raw .PST files and the other with the DII files. You should check the DII and .PST file names to match the DII file with its corresponding .PST files. Make sure that the DII file names match the .PST IDs, and make any necessary changes in the **eDiscovery Console**. You can then process the .PST files using the **eDiscovery Console** before loading the DII file. (For additional information, see the Batch Loading eDiscovery Processed by Service Bureau or Forensic Experts section in this white paper.)*

These steps make possible the production of eDiscovery in native format and to enable tracing the .PST and .NSF files back to their original sources.

Processing an Entire Volume

This section outlines the steps for one method of using the **eDiscovery Console**. Additional **eDiscovery Console** functionality is described in *The eDiscovery Console* appendix to this white paper. The following high-level steps are described in detail in this section:

1. Open the case that you want to load data into.
2. Choose the form or table that you want to load data into.
3. Open the **eDiscovery Console** to process the data.
4. Create a repository location.
5. Name the volume for storage on your system.



6. Select the authenticating volume, and enter comments about it.
7. Enter comments about individual .PST or .NSF files.
8. Copy the volume to your system.

In a real setting, you need to connect to an authenticating volume before following the procedure in this section. An authenticating volume is a storage device that came from your client, opposing counsel, or someone involved in the lawsuit, which contains electronic information being produced or made available for review and potential production. It can take various forms, such as a CD-ROM or a DVD that you can load directly into your computer, or a hard drive that can be connected to your computer.

For the purposes of this example, the authenticating volume consists of a set of files included with Summation Version 2.5 and later. If you have Summation Version 2.5 or later loaded, those files are located in the **eDocsSample** folder found in your Summation application directory.

Note: *When you receive an authenticating volume, make a complete copy immediately, preferably on a medium that cannot be modified later on. Store the original volume in a safe and secure location, and work with the copy.*

Use a unique name for each authenticating volume. If at all practical, include a unique identification number as part of the name. Maintain a log of the volume names and, in the log, include chain-of-custody information, such as:

- *The date you received the authenticating volume*
- *The name and contact information for the person from whom you received the volume*
- *Identification numbers of cover letters accompanying the volume*
- *The volume's medium (CD, DVD, hard drive, and so forth)*
- *Persons related to the volume (for example, the plaintiff's expert economist Dr. Benjamin Gompertz)*

Scan all files for viruses before loading them into Summation.

As early in the case as possible, try to resolve the question of the format or formats in which eDiscovery will be produced. The sooner you can come to an agreement with opposing counsel (or obtain an order from the court, if necessary), the more likely you will be able to determine the most effective and cost-efficient way to handle eDiscovery on your end.

To process a volume:

1. Launch Summation and open the case that you want to load data into by clicking the **Open Case** icon on the toolbar.
OR
From the **Case** menu, select **Open**.
The **Select a Case to Load** dialog box is displayed.
2. Highlight the case that you want to load data into and click **Select**. For the purposes of the example used throughout this white paper, select the case **P. Franc Vs. K. Morris**.
The case is opened.



- From the **File** menu, choose **Select Form**.
The **Choose New Form to Load** dialog box is displayed. You can select the type of form that you want to use when loading information. If your case includes eDiscovery, Summation recommends that you use the **E-form/E-table**. You can use a custom form, but it is important to ensure that you have enough fields to accommodate all eDiscovery *metadata*.

*NOTE: When you create a new case (from the **Case** menu, select **New**, and the **Start A New Case** dialog box is displayed), you can apply the **E-form** to any new case involving electronic evidence by selecting the **Use E-form for eDocs & eMail** check box. By default, this option is selected.*

- Select **E-form/E-table** and click **Load Form**.
The form is set in the background to receive data.
- Click the **Case Explorer** pane to bring it into focus, and, from the **File** menu, select **Process eDiscovery...**
The **eDiscovery Console** is displayed. By default, the **Process Entire Volume** tab is displayed topmost. Figure 1 shows the **eDiscovery Console**. The following Steps in this procedure refer the lettered items on this tab.

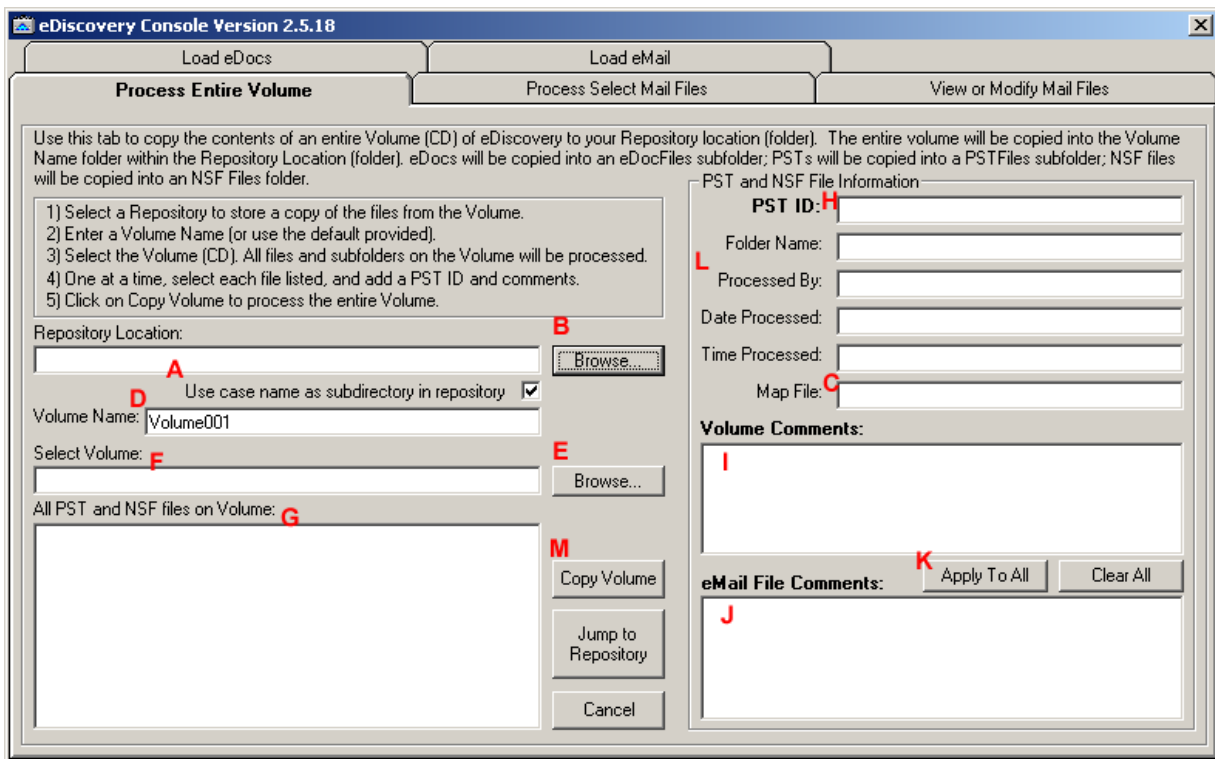


Figure 1: eDiscovery Console, Process Entire Volume Tab

- Click **Browse** (Figure 1, B) next to the **Repository Location** field.
The **Browse for Folder** dialog box is displayed.
- Select the location where you want Summation to load the contents of your authenticating volume, and click **OK**.
The path is displayed in the **Repository Location** field. For example, **U:\eDiscoveryRepository**. In addition, the **Map File** (Figure 1, C) field is populated with this path.



*NOTE: Do not load the contents of your authenticating volume within the Summation application, **CaseData**, or **Cases** directories, or any subdirectories within them.*

8. Click the **Use case name as subdirectory in repository** check box (Figure 1, A) to automatically create a subdirectory using the case name and append the subdirectory to the path. For example **U:\eDiscovery Repository\P. Franc Vs. K. Morris**.

OR

Type the name the subfolder you want to use for the case.

*NOTE: By clicking the **Use case name as subdirectory in repository** option, all case information is stored in an easily identifiable folder. This allows you and others working with the case to access data with minimal confusion.*

9. In the **Volume Name** field (Figure 1, D), type the name that you want to assign to the authenticating volume.

NOTE: It is recommended that you use the same name for the volume on your computer as is used by the authenticating volume (the physical evidence). This way, you improve your ability to quickly refer to the original copy of the data when necessary.

10. Click **Browse** next to the **Select Volume** field (Figure 1, F), select the authenticating volume, and click **OK**. For the purposes of this example, use the **eDocsSample** folder in your Summation application directory. In a real setting, you would connect your authenticating sample to your computer prior to launching Summation.

The volume path is displayed in the **Select Volume** field, and the names and paths for .PST and .NSF files are displayed in the **All PST and NSF files on Volume** field. Note that this is for informational purposes only, and no data is copied during this step.

In addition, the **eDiscovery Console** auto-populates the **PST ID** field (Figure 1, H) for each .PST and .NSF file. Summation requires that each .PST and .NSF file in a case have a unique identifier. The auto-assigned **PST ID** is comprised of two parts: the name of the .PST or .NSF file and the date that the .PST or .NSF file was processed. For example, the **PST ID** for the **CStevens** .PST file might be **CStevens_Jan30_2004**. To see the **PST ID** for a file, click the file name in the **All PST and NSF files on Volume** field.

The **eDiscovery Console** does not write the PST ID to the database at this point, which gives you the opportunity to manually change it.

NOTE: Unless you have a compelling reason to change the **PST ID**, use the one that the **eDiscovery Console** automatically assigns. This way, you can use the **PST ID** to monitor both source and load data.*

11. Type any comments you have about the volume in the **Volume Comments** field (Figure 1, I), if you would like to do so. This Step is optional.

* A compelling reason to change the **PST ID** occurs when the service bureau processing a Microsoft Outlook .PST file and creating a DII (load) file assigns a file name to the .PST and DII files that differ from the **eDiscovery Console** default. In such a situation, you may want to rename the **PST ID** to match the source (for example, if the DII file is named **CStevensOne.DII** and .PST file name is **CstevensOne.PST**, then populate the **PST ID** field with **CstevensOne**).



12. Type any comments you have about that pertain to individual .PST or .NSF files, if you would like to do so. This Step is optional.
13. Select the file for which you want to save comments and type the comments in the **eMail File Comments** field (Figure 1, J). Click **Apply to All** (Figure 1, K) to save those comments to all the files. Otherwise, your comments are saved to the individual file with no further action.
14. Click **Copy Volume** (Figure 1, M).
The **eDiscovery Console** auto-populates additional .PST and .NSF information in the **PST and NSF File Information** fields: **Folder Name**, **Processed By**, **Date Processed**, and **Time Processed** (Figure 1, L). The **eDiscovery Console** copies all .PST files into the **PSTFiles** folder, all .NSF files into the **NSFFiles** folder, and all remaining electronic files into the **eDocsFiles** folder in the repository you chose in Step 7. The **eDiscovery Console** maintains the original directory structure as it appeared on the authenticating volume.

In addition, the **eDiscovery Console** removes the read-only attribute from .PST and .NSF files, and collects additional information from the .PST and .NSF files to facilitate production of individual e-mail messages from the original authenticating location.

15. Click **Jump to Repository** to check the copied contents.
The Microsoft **Windows Explorer** window is displayed, showing the directory of your volume.

*NOTE: If a .PST file is password protected, the **eDiscovery Console** will not be able to open and load it. You are notified that the .PST file could not be opened and the errors are written to a log file (located at: **C:\iBlaze25\CaseData\). To load a password protected .PST file, open it in Microsoft Outlook first using the password, if you know it. If you do not know the password, then you may want to consider using a service bureau to process your electronic documents for this case.***



Loading eDiscovery

Summation Blaze LG Gold and iBlaze include built-in utilities for loading eDiscovery. You can use these utilities to load e-mail messages and electronic documents from volumes that you receive, or you can opt to have a service bureau batch process files for you (the latter is covered in greater detail in the *Batch Loading eDiscovery Processed by Service Bureaus or Forensic Experts* section of this white paper).

Reasons to Load eDiscovery with the Built-in Summation Utilities

There are many reasons why you might want to use the Summation utilities instead of sending the work to a service bureau:

- The files you need to work with are in common formats supported by Summation, such as .PST files, Microsoft Word files, and Microsoft Excel files.
- The files you need to work with include unusual types that you nonetheless have the ability to convert to a format Summation can process. For example, you might be able to load Eudora or GroupWise files into Microsoft Outlook, convert them to .PST files, and load the converted files into Summation.
- You have Quick View Plus and plan to use it with Summation to view file formats that Summation's **eDocs Viewer** is not designed to handle. You can use QuickView Plus to save the files to formats that Summation can index, or *petrify* a limited number of electronic documents into the Tagged Image File Format (.TIFF) images that you can then load into Summation.
- You have Adobe® Acrobat® and plan to use it to convert electronic documents that are in formats not supported by Summation to .PDF files.
- Your client pre-processed some of the eDiscovery, taking care of tasks such as removing encryption and duplicates, and sent you files ready to load into Summation.
- You have budgetary concerns, client directives, or other reasons.

Note: *Searching and reviewing native electronic file information, whether processed and loaded through the **eDiscovery Console**, or processed by a service bureau and loaded with the Summation DII (DII) file, is easy. You can use the Summation **Case Explorer** search as you do for any other case element (such as transcripts or notes). However, it is important to know your limits, especially when determining who processes, loads, produces and, otherwise works with eDiscovery. If you are uncertain about how to work with the electronic files you receive in discovery, consider getting assistance from others with more experience in this area. Your organization may have a litigation support or practice support group that you can consult. Summation maintains a list of trainers on its web site: <http://www.summation.com/training/>. In addition, many service bureaus can provide help as can independent eDiscovery advisors. For a partial listing, see <http://www.sochaconsulting.com/vendors.htm>.*

Loading Microsoft Outlook E-mail Messages and E-mail Attachments

Now that electronic documents, e-mail messages, and e-mail attachments have been processed successfully with the **eDiscovery Console**, you are ready to load the eDiscovery documents. This section discusses loading e-mail messages (specifically .PST files) and e-mail attachments, and the following section discusses loading electronic documents.



The following high-level steps are described in detail in this section:

1. Open the case into which you want to load data, open the **eDiscovery Console** and select the **Load eMail** tab.
2. Review the **Core Database** fields into which the **eDiscovery Console** will populate e-mail information, and make any necessary changes.
3. Select the type of e-mail messages that you want to load.
4. Select the e-mail folder that you want to load.
5. Specify the location where you want to load e-mail message body.
6. Specify whether you want to load e-mail attachments.
7. Specify whether you want to process .MSG attachments.
8. Set a date range for the e-mail messages and attachments that you want to load.
9. Name the load session.
10. Assign a document starting number.
11. Load the e-mail messages and attachments.

Note: To load .PST files successfully into Summation, Microsoft Outlook must be installed on the workstation you are using to load e-mail messages. Microsoft Outlook must also be set up as the default mail client while loading, but can be changed after the load process is complete.

When Summation is installed on a laptop that is generally connected to a network, and Microsoft Outlook is set up to run from a Microsoft Exchange server, you must set up a local Microsoft Outlook profile to load e-mail messages while away from the office (and not connected to the Microsoft Exchange server). For assistance with setting up a local profile, see your IT department or the Help included with Microsoft Outlook.

You can use the **eDiscovery Console** to load .PST and .NSF files. At this time, however, Summation has not added the ability to produce .NSF files.

To load e-mail messages and e-mail attachments using the **eDiscovery Console**:

1. Launch Summation and open the case into which you want to load data by clicking the **Open Case** icon on the toolbar.
OR
From the **Case** menu, select **Open**.
The **Select a Case to Load** dialog box is displayed.
2. Highlight the case into which you want to load data and click **Select**. For the purposes of the example used throughout this white paper, select the case **P. Franc Vs. K. Morris**.
The case is opened.
3. From the **File** menu, choose **Select Form**.
The **Choose New Form to Load** dialog box is displayed. You can select the type of form that you want to use when loading information. If your case includes eDiscovery, Summation recommends that you use the **E-form/E-table**. You can use a custom form, but it is important to ensure that you have enough fields to accommodate all eDiscovery metadata.



NOTE: When you create a new case (from the **Case** menu, select **New**, and the **Start A New Case** dialog box is displayed), you can apply the **E-form** to any new case involving electronic evidence by selecting the Use **E-form for eDocs & eMail** check box. By default, this option is selected.

4. Select **E-form/E-table** and click **Load Form**.
The form is set in the background to receive data.
5. Click the **Case Explorer** pane to bring it into focus, and, from the **File** menu, select **Process eDiscovery...**
The **eDiscovery Console** is displayed. Select the **Load eMail** tab.

OR

From the **File** menu, select **Load Documents** and **Load eMail...**
The **eDiscovery Console** is displayed with the **Load eMail** tab topmost. The **Load eMail** tab is shown in Figure 2. The following Steps in this procedure refer to the lettered items on this tab.

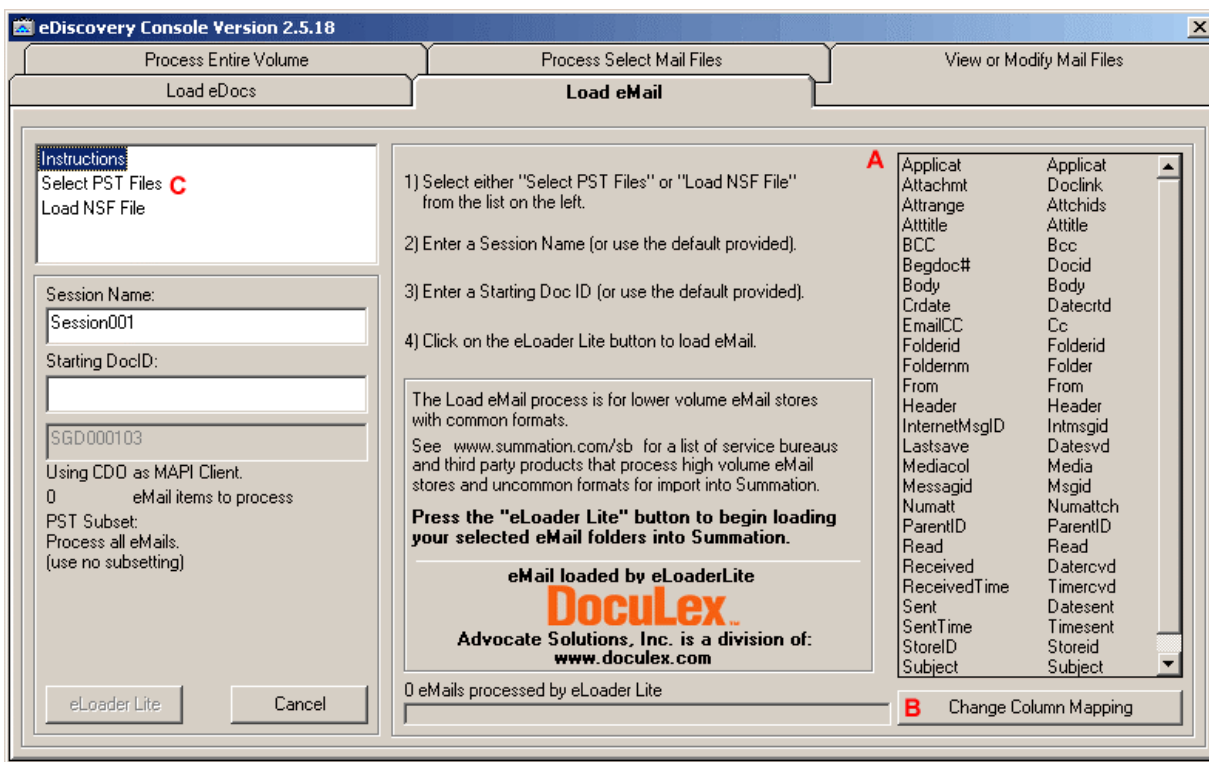


Figure 2: eDiscovery Console, Load eMail Tab

6. Review the list of **Core Database** fields (Figure 2, A) that the **eDiscovery Console** auto-populates with e-mail information.
7. If necessary, click **Change Column Mapping** (Figure 2, B) to modify fields according to your needs.
The **Defaults** dialog box is displayed, listing e-mail-related fields and their corresponding **Core Database** fields, which are populated with e-mail metadata.
8. Click the drop-down menu for the column mapping that you want to change, and assign a new database field to the column. Click **OK** when you are finished changing mappings.
Your changes are saved, and the **eDiscovery Console** is redisplayed. Your changes are reflected in the list of fields.



9. Select the type of e-mail messages that you want to load into Summation (Figure 2, B). For this example, click **Select PST Files** to load Microsoft Outlook files. The **Select PST Files to Load** area is displayed in the center of the **eDiscovery Console**, showing an e-mail tree that lists the .PST files that were processed with the **eDiscovery Console**. Figure 3 shows the **Load eMail** tab at this point in the procedure. The following Steps in this procedure refer to the lettered items on this tab.

*NOTE: If the .PST files that you want to load are not displayed in the e-mail tree, click **Add eMail Files** (Figure 3, C) and select additional processed .PST files to include in your tree. Click **OK** when you are finished.*

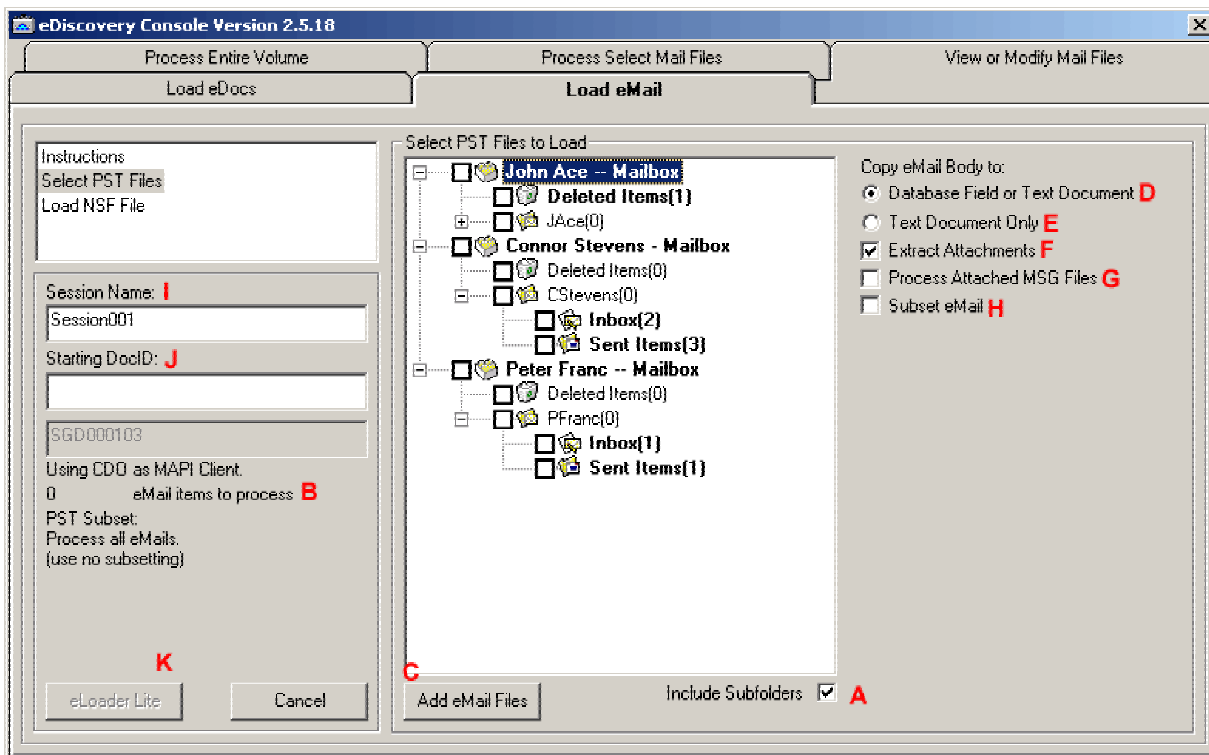


Figure 3: eDiscovery Console, Select PST Files to Load

10. In the e-mail tree, select the folders containing the e-mail messages that you want to load into Summation. You can select any combination of folders and subfolders. To include all subfolders, click the **Include Subfolders** check box. The **eDiscovery Console** displays the number of **eMail items to process** (Figure 3, B). For the example scenario, click **Include Subfolders** and select **Connor Stevens – Mailbox**. Then, clear the **Deleted Items** check box.

*NOTE: As a general rule, use the **Include Subfolders** option (Figure 3, A). Selecting this option significantly reduces the risk of failing to load relevant e-mail messages. If you do not load a message, you cannot review, evaluate, or produce it. If you know that you are only interested in the contents of specific folders or if you need to reduce the volume of data to load and search, do not use this option.*



11. In the **Copy eMail Body to** list, select the method(s) that Summation should use to load the e-mail messages. You can choose from the following options:
- **Database Field or Text Document** – Saves the text of the e-mail message body into the **Body** field in the **Core Database**. If the body of the e-mail message exceeds 28,000 characters, the additional characters are stored in a text file. The text file is saved in the case directory: **X:\<Summation Application Directory>\CaseData\<Case Directory>\eDocs\emb\<Session Name>**. The text file is linked to the database summary. This option is selected by default. (Figure 3, D)
 - **Text Document Only** – Saves the text of all e-mail messages as text files. (Figure 3, E)
 - **Extract Attachments** – Loads e-mail attachments into Summation. This option is selected by default. (Figure 3, F)
 - **Process Attached MSG Files** – Loads .MSG files attached to e-mail messages as e-mail messages.
 - **Subset eMail** – Sets a date range for e-mail messages and attachments to load. By default, this option is not selected, and all e-mail messages and attachments from the selected folders are loaded. If you select this option, date range options are displayed. Figure 4 shows these options.

The image shows a dialog box titled "Subset eMail". At the top left, there is a checked checkbox labeled "Subset eMail". Below this, there are two main sections. The first section is titled "By Received Date" and has an unchecked checkbox. It contains two date pickers: "From:" with the value "1 / 1 /1994" and "To:" with the value "2 / 2 /2004". Below these are two radio buttons: "AND" (which is selected) and "OR". The second section is titled "By Sent Date" and also has an unchecked checkbox. It contains two date pickers: "From:" with the value "1 / 1 /1994" and "To:" with the value "2 / 2 /2004".

Figure 4: Subset eMail Options

12. If you selected **Subset eMail** in Step 11, specify **By Received** and/or **By Sent Date** ranges. You can set date options in four different ways:
- Select **By Received Date** and enter beginning and ending dates to load e-mail messages and attachments received between the specified dates.
 - Select **By Sent Date** and enter beginning and ending dates to load e-mail messages and attachments sent between the specified dates.



- Select **By Received Date, By Sent Date, and AND**, and enter date ranges for both options to load e-mail messages and attachments that were sent between the specified dates and received between the specified dates.
- Select **By Received Date, By Sent Date, and OR**, and enter date ranges for both options to load e-mail messages and attachments that were sent between the specified dates or received between the specified dates.

Click the drop-down arrows in the date fields to display a calendar. To change the year, click the year and use the resulting arrows to move to the year you want to set. To change the month, use the arrows to the left or right of the month displayed, or click the month directly and choose the month you want from the menu that is displayed. To set a specific day, click that day on the calendar.

The dates you specify are displayed in the bottom left area of the **eDiscovery Console**, as shown in Figure 5.

```
Using CDO as MAPI Client.  
11      eMail items to process  
PST Subset:  
Rcv'd Between 1/1/1994 and 2/2/2004  
AND  
Sent Between 1/1/1994 and 2/2/2004
```

Figure 5: Subset Dates

13. In the **Session Name** field (Figure 3, I), type a descriptive name for your load session. For this example, type the following:

```
Client eMail
```

14. In the **Starting DocId** field (Figure 3, J), type a prefix or starting document number that the **eDiscovery Console** will use to assign sequential document numbers to the e-mail messages and attachments it loads. For this example, type the prefix the following prefix, since you are loading Connor Stevens's e-mail messages and attachments.

```
CS
```

If the prefix that you specify does not exist in the database for your case, the **eDiscovery Console** displays the prefix you entered and starts the count at 1.

If the prefix that you specify exists in the database for your case, the **eDiscovery Console** displays the next available number for that prefix.

*NOTE: In general, avoid using the letters **I** and **O** in prefixes, as they are easy to confuse with **1** and **0**. However, use **I** and **O** if it gives greater clarity to your prefix, as in **EMAIL000001** or **EDOCS000001** (where **EMAIL** and **EDOCS** are prefixes containing these letters).*

*The **eDiscovery Console** automatically converts all letters to upper case, regardless of whether you use lower case or upper case letters in your prefix.*

15. Review your settings to ensure they are correct and click **eLoader Lite** (Figure 3, K) to load the e-mail messages and attachments. The e-mail messages and attachments are loaded. The **eLoader Lite** dialog box is displayed, giving you the option to process additional discovery or return to Summation.



16. For this example, click **Return to Summation**.
The **Summation Blaze LG** dialog box is displayed. You must *Blaze* (when you Blaze the database, a vocabulary list is generated, allowing faster searches) the database in order to search the electronic documents that you loaded.
17. Click **Yes**.
The e-mail messages and attachments are Blazed and can now be searched.

Loading Electronic Document Files

Once you have processed your electronic discovery and loaded your e-mail messages and attachments, you are ready to load the electronic documents that you received in the case. This section explains how to load electronic documents.

The following high-level steps are described in detail in this section:

1. Open the case that you want to load data into, open the **eDiscovery Console**, and select the **Load eDocs** tab.
2. Select the folder containing the electronic documents that you want to load.
3. Select the electronic documents that you want to load.
4. Assign a document starting number.
5. Load the electronic documents.

To load electronic document files using the **eDiscovery Console**:

1. Launch Summation and open the case that you want to load data into by clicking the **Open Case** icon on the toolbar.
OR
From the **Case** menu, select **Open**.
The **Select a Case to Load** dialog box is displayed.
2. Highlight the case that you want to load data into and click **Select**. For the purposes of the example used throughout this white paper, select the case **P. Franc Vs. K. Morris**.
The case is opened.
3. From the **File** menu, choose **Select Form**.
The **Choose New Form to Load** dialog is displayed. You can select the type of form that you want to use when loading information. If your case includes eDiscovery, Summation recommends that you use the **E-form/E-table**. You can use a custom form, but it is important to ensure that you have enough fields to accommodate all eDiscovery metadata.

*NOTE: When you create a new case (from the **Case** menu, select **New**, and the **Start A New Case** dialog box is displayed), you can apply the **E-form** to any new case involving electronic evidence by selecting the Use **E-form for eDocs & eMail** check box. By default, this option is selected.*

4. Select **E-form/E-table** and click **Load Form**.
The form is set in the background to receive data.



- Click the **Case Explorer** pane to bring it into focus, and, from the **File** menu, select **Process eDiscovery...**
The **eDiscovery Console** is displayed. Select the **Load eDocs** tab.
OR
From the **File** menu, select **Load Documents** and **Load eDocs...**
The **eDiscovery Console** is displayed with the **Load eDocs** tab topmost.
- Click **Browse** to select the folder containing the electronic documents that you want to load.
The **Browse for Folder** dialog box is displayed.
- Navigate to the location where you copied the authenticating volume when you processed the eDiscovery, select the folder containing the electronic documents that you want to load, and click **OK**.
A list of the files in the folder is displayed. Figure 6 shows the **Load eDocs** tab with the files listed. The following Steps in this procedure refer the lettered items on this tab.

*NOTE: It is recommended that you load at the lowest subfolder level rather than loading the entire volume. That way, you will not needlessly load .PST or .NSF files that were processed and loaded separately. In this example, navigate to **U:\eDiscovery Repositories\P. Franc Vs. K. Morris\Volume 001\EDocFiles\Edocs**.*

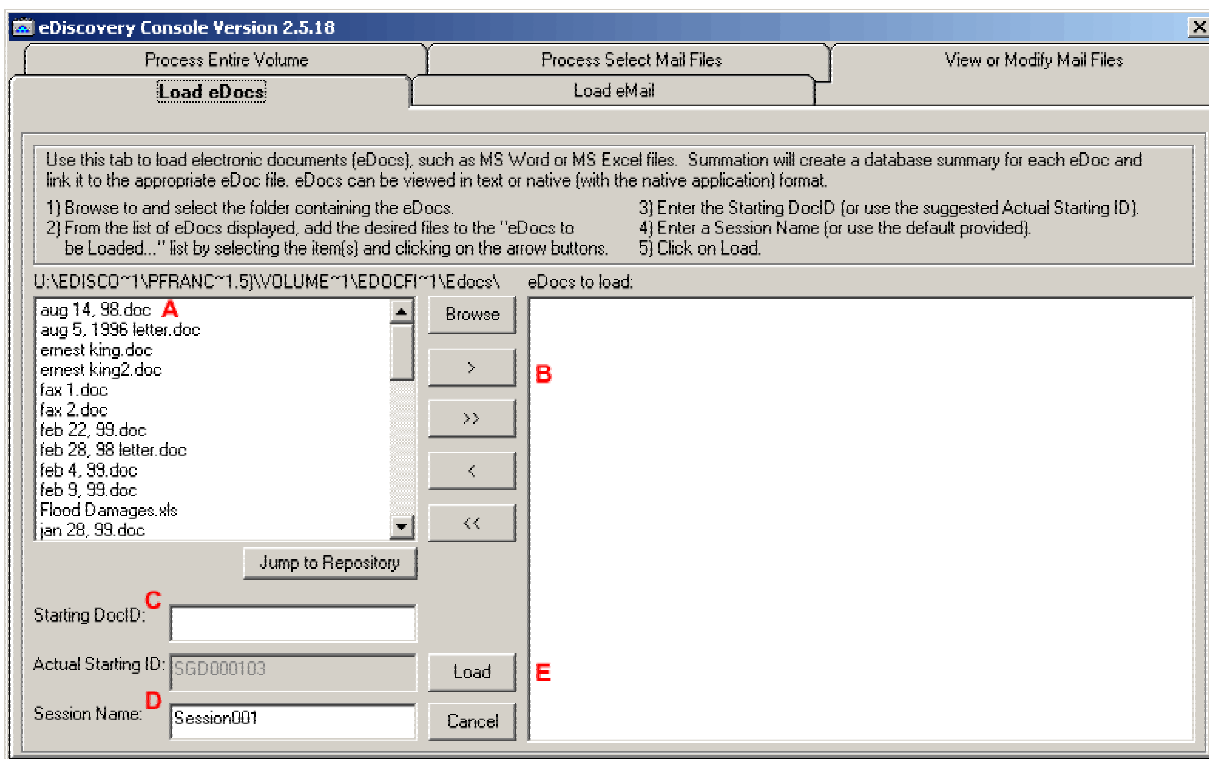


Figure 6: eDiscovery Console, Load eDocs Tab



8. To load a single file, select the file and click **>** (Figure 6, B).

OR

To load all files, click **>>**.

OR

To load selected sequential files, select the first file, press your **Shift** key, and select the last file in the group. Then, click **>**.

OR

To load selected non-sequential files, press your **Ctrl** key while selecting the files. Then, click **>**.

The selected files are listed in the **eDocs to load** box.

NOTE: You can load the entire contents of multiple folders by browsing to each folder and selecting it. Selecting multiple folders to load at once does not allow you to assign individual files from those folders to load, but will load the entire contents of all selected folders.

*To remove files from the **eDocs to load** list, select the files and click **<**. To remove all files from the list, click **<<**.*

9. In the **Starting DocId** box (Figure 6, C), type a prefix or starting document number that the **eDiscovery Console** will use to assign sequential document numbers to the electronic documents it loads. In the example shown in Figure 6, documents numbered SGD000001 to SGD000102 were already used in the database, so the **eDiscovery Console** displays the next available number with that prefix, SGD000103, in the **Actual Starting ID** box.

If the prefix that you specify does not exist in the database for your case, the **eDiscovery Console** displays the prefix you entered and starts the count at 1.

If the prefix that you specify exists in the database for your case, the **eDiscovery Console** displays the next available number for that prefix.

*NOTE: In general, avoid using the letters **I** and **O** in prefixes, as they are easy to confuse with **1** and **0**. However, use **I** and **O** if it gives greater clarity to your prefix, as in **EMAIL000001** or **EDOCS000001** (where **EMAIL** and **EDOCS** are prefixes containing those letters).*

*The **eDiscovery Console** automatically converts all letters to upper case, regardless of whether you use lower case or upper case letters in your prefix.*

10. In the **Session Name** box (Figure 6, D), type a descriptive name for your load session. For this example, type the following:

```
Client eDocs
```

11. Review your settings to ensure they are correct and click **Load** (Figure 6, E) to load electronic documents.

A status dialog box is displayed.

12. When loading is complete, click **OK**.

The **eDiscovery Console** is redisplayed.

13. Close the **eDiscovery Console**.

The **Summation Blaze LG** dialog is displayed. You must Blaze the database in order to search the electronic documents that you loaded.

14. Click **Yes**.

The documents are Blazed and can now be searched.



Note: If the repository contains password protected electronic files, **the eDiscovery Console** copies the files to the **Case** directory without Blazing them (as they cannot be opened). When you attempt to view the files in their original formats in Summation, you are prompted for a password.

Summation recommends that you use a service bureau to process and load password protected files, as service bureaus are better equipped to crack open the files.

Batch Loading eDiscovery Processed by a Service Bureau or Forensic Experts

Rather than loading eDiscovery yourself, you can contact a service bureau for assistance. Using a service bureau to process eDiscovery has distinct advantages. Service bureaus are equipped to handle eDiscovery at a level that most law firms cannot match. For example, they can:

- Process a larger volume of eDiscovery more efficiently than a law firm using Summation's loading utilities, especially if the firm does not have the human or technological resources to devote exclusively to processing and loading eDiscovery.
- Petrify a large volume of electronic documents into PDF or TIFF formats more efficiently than a law firm using the Summation utility.
- Process a larger range of electronic file formats than the processor built into Summation is designed to handle, such as older or rare e-mail store types. (See the list of supported file formats in the *Electronic File Formats Supported by Summation's Native Indexer* appendix to this white paper.)
- De-duplicate eDiscovery, so that multiple copies of an e-mail message or an electronic document will be included in the database only once, but will nonetheless be tracked for other purposes.
- Extract metadata from e-mail messages and electronic documents beyond the amount that Summation's utility captures, and process that information for loading into the Summation **Core Database**.
- Un-encrypt or bypass passwords on protected files.
- Check large volumes of eDiscovery for viruses.
- Avoid common eDiscovery processing errors, such as inadvertently altering metadata and other parts of e-mail messages and electronic documents, failing to capture all relevant information, or improperly handling data from legacy systems.
- Provide a single load file for paper and electronic documents, so that you only have to go through one load process.

Note: *Selecting and working with a service bureau can be an intimidating process for those who have not done it before. If you are new to this process, consider getting assistance from others with more experience in this area. Your organization may have a litigation support or practice support group that you can consult. Even absent a formal group, your organization may have people who have been through the process and can provide guidance. For larger or more complex matters, you might want to turn to an independent consultant.*

You can also ask service bureau personnel for help, but you should not treat their recommendations as impartial advice.



When selecting a service bureau, make sure that you know what they intend to deliver to you. Some service bureaus are set up to deliver eDiscovery in its native format, or as close to its native format as is practical. Others are structured to deliver eDiscovery as either as TIFF or PDF files that are generally accompanied by some of the metadata associated with the eDiscovery.

De-duplication, offered by many service bureaus, can greatly reduce the volume of eDiscovery that you ultimately process. You can end up with a smaller, and thus more manageable, set of discovery materials. You should also be able to reduce processing and handling costs considerably.

If you choose to have a service bureau de-duplicate eDiscovery, make sure that you understand the processes used by that service bureau. You should avoid de-duplication processes that are overly exclusive and that eliminate as duplicates those files that, for the purposes of your lawsuit, should not be treated as duplicates. You should also find out the type of tracking and recovery mechanisms that are available, in the event that you need to go back and produce materials that you initially considered to be duplicates but can no longer treat as such.

Metadata, such as the creation date and time of an electronic document, may be largely irrelevant in some cases, but in other situations, it can be nearly as important as the document itself. As early in the process as you can, try to determine what metadata you want from your eDiscovery, what you would like to do with the metadata, and the format that you want the service bureau to use to deliver the metadata.

If you opt to have a service bureau process your eDiscovery, the service bureau will provide you with a Summation load file, known as a *DII* (Document Image Information) file, to batch load eDiscovery.

Summation uses eDII files to batch load electronic, imaged, and full-text documents processed by service bureaus. To accommodate loading eDiscovery processed by service bureaus, Summation has extended the DII file format used in Summation versions prior to Version 2.5. The DII file format includes all previous tokens and formats, as well as additional ones to specifically handle eDiscovery documents and metadata (these additional tokens are listed in *The DII Load File* appendix to this white paper).

Note: Before you load a DII file from a service bureau that has prepared eDiscovery for you, Summation recommends that you process the eDiscovery using the **eDiscovery Console**. This is especially important if you intend to produce electronic documents, e-mail messages, and e-mail attachments in electronic format. For further details, see the Processing eDiscovery section of this white paper.

To load the DII file and discovery documents:

1. Open the DII file in a text editor and verify the following information:
 - In the **@eDOC** token, verify that the electronic documents exist in the location indicated. Summation needs the electronic document files in this location so that it can locate and copy them into the **eDocs** folder.
 - In the **@FULLTEXTDIR** token or the **@D** token, verify that the full-text files exist in the location indicated. Summation needs the full-text files in this location so that it can locate the full-text files and copy them to the *ocrBase* (the Summation module that permits the loading and searching of full-text versions of imaged documents).
2. Open the case that you want to load the DII file into.



3. From the **Options** menu, select **Defaults**.
The **Defaults** dialog box is displayed.
4. Click the **Imaging** tab. Figure 7 shows the **Imaging** tab. The following Steps in this procedure refer the lettered items on this tab.

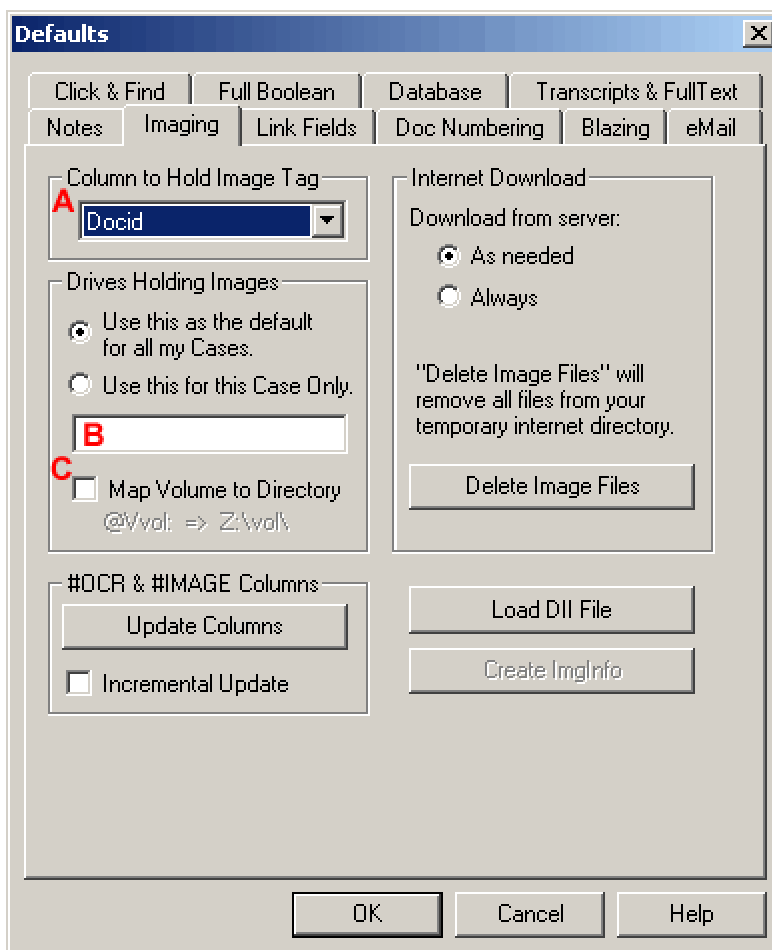


Figure 7: Defaults Dialog Box, Imaging Tab

5. In the **Column to Hold Image Tag** menu (Figure 7, A), select the field that you want to be the common link between the images and the document database. By default, **DocID** is used for the **E-table** (if you have the **E-form** loaded) and **Begdoc#** is used for the **Stdtable** (if you have the **Stdform** loaded).

NOTE: You are not forced to use the default fields designated by Summation. You can use any note-type or text-type field, including a custom field.



6. If you are going to copy and view images from a network location, leave the **Drives Holding Images** (Figure 7, B) field empty and make sure that the **Map Volume to Directory** (Figure 7, C) option is not checked.

OR

If you are going to view the images from your CD-ROM drive, and the **Imginfo** table references **@V** (this is referenced in the DII file by the **@D** token) in the image path, enter the name of the drive containing the images in the **Drives Holding Images** (Figure 7, B) field and leave the **Map Volume to Directory** check box (Figure 7, C) clear.

OR

If you are going to view the images from your CD-ROM tower, and the **Imginfo** table references **@V** (this is referenced in the DII file by the **@D** token) in the image path, enter the name of the drive containing the images in the **Drives Holding Images** (Figure 7, B) field and check the **Map Volume to Directory** option (Figure 7, C).

NOTE: If you store images on the network, it is best to store them in a location other than the location where the case data is stored. This allows the server where the case data is stored to perform more efficiently (for example, backups will process more efficiently and space is not consumed by static data, such as discovery documents).

7. Click **Load DII File**.
The **Read DII File** dialog box is displayed.
8. Click **Browse**.
The Choose **the DII File to Be Loaded** dialog box is displayed.
9. Navigate to the file you want to load, select it, and click **Open**.
The **Read DII File** dialog box is redisplayed.
10. If your file includes either e-mail messages or electronic documents, click the **Look for eDiscovery** option.
11. Click **OK**.
The **Electronic Document Information** dialog box is displayed.
12. If your file includes either e-mail messages or electronic documents, type a session name in the **eDoc Session Name** box. For this example, type **Client Authenticating Volume**.
13. If your file includes e-mail messages from a .PST or an .NSF file, select the **PSTID** for the originating e-mail file from the **PST (Store) ID** menu. For example, select **CStevens_Jan30_2004**.
14. Click **OK**.
The electronic documents, e-mail messages, and e-mail attachments are loaded into Summation and the image information is written to the **Imginfo** table in the **Core Database**. When loading is complete, Summation Blazes the added items.

Note: *The following items must be Blazed before they can be searched: electronic documents, e-mail attachments, and the entire **ocrBase**. The following items can be searched without Blazing: e-mail messages (if they have been loaded into a field in the database), individual **ocrBase** documents (as opposed to the entire **ocrBase**), and data in the **Core Database**. Summation recommends that you Blaze your cases regularly to allow faster searching.*



Searching and Reviewing eDiscovery

After you or your litigation manager have successfully processed and loaded eDiscovery into your Summation case, you are ready to begin searching, reviewing, and analyzing the eDiscovery materials (including any scanned and coded paper discovery) that were loaded into the case. Summation's standard search, sort, zoom, and display features help you in this phase.

The Summation Blaze engine indexes the text in e-mail messages and electronic documents, allowing you to search any combination of the following items:

- The body of eDiscovery documents, such as electronic documents, e-mail messages, and e-mail attachments
- Coded information in the database summaries associated with eDiscovery, including any captured metadata
- Both of the above in conjunction with other case information

This section describes how to execute a search and review search results that are relevant to the opposing counsel's request for production. As will be explained, you can search for terms in multiple types of electronic discovery. In the example used in this section, you will perform a search using the search string **flat space OR flood** in the following case items:

- **Core Database** – Coded information about paper and eDiscovery documents
- **ocrBase** – Text of paper discovery
- **eDocs** – Text of electronic documents
- **eMail** – Text of e-mail messages
- **eMail Attachments** – Text of e-mail attachments

Note: *One of the most effective ways to search through case elements is to use an iterative search process involving the following steps:*

1. *Define an issue.*
2. *Develop a set of search criteria.*
3. *Apply the criteria to information available about the documents, whether they are paper or electronic. If this does not result in a list of documents, return to Step 2.*
4. *Retrieve the designated documents.*
5. *Start reviewing the retrieved documents.*
6. *If necessary, return to Step 2 to redefine search criteria.*

The following information explains how to perform a search.

To perform a search:

1. Open the case **P. Franc Vs. K. Morris** in your **Case Explorer**, if it is not already open.
2. From the **View** menu, select **Show** and **Docked Explorer Layout**. Your layout is set with the **Case Explorer** on the left. Other open views will be shown with tabs on the right. Tabs are displayed along the bottom.



3. In the **Case Explorer**, select the following items for searching, as shown in Figure 8:

- **Core Database**
- **ocrBase**
- **eDocs**
- **eMail**
- **eMail Attachments**

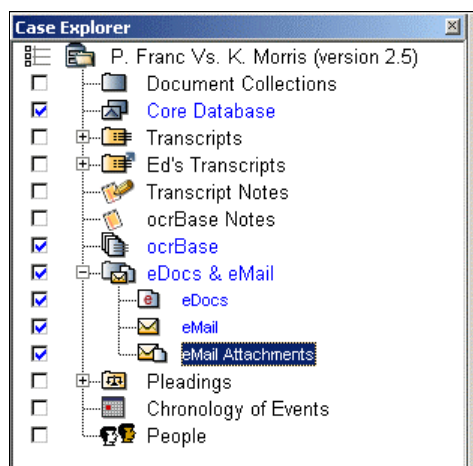


Figure 8: Case Elements to Search

4. In the **Search** box, type the following search string, and click **Search**.

flat space OR flood

The **Search Results** page is displayed, listing all documents that contain the either the phrase “flat space” or the word “flood.”

5. Review the excerpts and summaries on the **Search Results** page. (For information about navigating the **Search Results** page, see the Help included with Summation.)

The following information explains how to adjust your display so that you can see several elements at once. This method of display is just a suggestion. As you work with Summation, you may find other ways of displaying the various elements that work better for you.

To adjust your display to show multiple elements:

1. Double-click the **Core Database** in the **Case Explorer**.
The database is opened in column view.
2. Double-click the **eDocs Viewer** in the **Case Tools** area of the **Case Explorer**.
The first electronic document in the case is displayed in the **eDocs Viewer**.
3. Right-click the title bar of the **eDocs Viewer**, select **Doc View**, and select **Right**.
Your view now displays the **Case Explorer** on the left, the **Core Database** column view in the middle, and the **eDocs Viewer** on the right. This setup facilitates the review of both the eDiscovery documents and associated database summary. You can also set the **Image Viewer** in this way to review images.



- Click a database record.
The document associated with that record is shown in the **eDocs Viewer**. If the document has an image associated with it, it is shown in the **Image Viewer**, if you have the **Image Viewer** open.

While reviewing documents, it is often helpful to see the parent/child relationships between documents. For example, if an e-mail message has attachments, the e-mail message is the parent and the attachments are the children. Figure 9 illustrates this relationship.

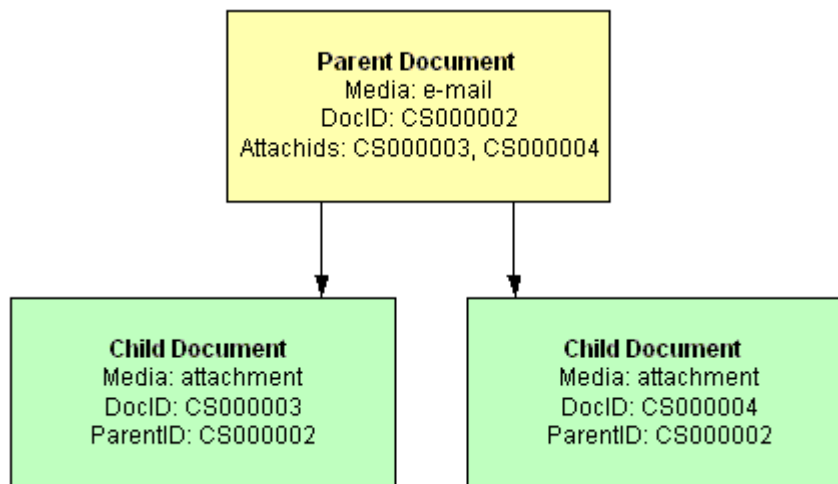


Figure 9: Parent/Child Relationship

The Summation **E-Table** tracks document relationships using the **DocID** (the unique document identifier) for each document in conjunction with the **Attachids** and **Parentid** fields. The **Attachids** field contains the **DocID**(s) that identify the attachments associated with a document. The **Parentid** field contains the **DocID** of the parent document. Figure 10 shows how this looks in the column view.

Note: If you use a service bureau to create a DII file to load eDiscovery, the DII file must be set up to populate the appropriate **Attachids** and **Parentid** fields.

Column E-table Display: Summary 3 of 11				
<i>Fields</i>	Docid	Media	Attchids	Parentid
7	CS000001	eMail		
8	CS000002	eMail	CS000003 CS000004	
9	CS000003	eMail		CS000002
10	CS000004	eMail		CS000002
11	CS000005	eMail		

Figure 10: Showing the Parent/Child Relationship in the E-table

Note: You can add fields to your column display by right-clicking the **Fields** heading on the column and dragging the fields that you want into the table.



To show document relationships among e-mail messages and attachments:

1. Click the **Core Database** column view to bring it into *focus* (bringing a view into focus means making that view active; the view that is in focus has a blue title bar, while other views have a gray title bar).
2. From the **Search** menu, select **Include Family Summaries**. This option allows you to see the relationship between documents.
The **Include Family Summaries** dialog box is displayed, allowing you to set the options you want to display.

NOTE: It is recommended that you include all family summaries in the document set when you review it for production. That way, the document set under review reflects the complete compound document (parent and children).

3. Select the options that you want to display and click **Yes**.
4. Double-click **eMail** in the **Case Explorer**.
The column view displays the e-mail records. Use the **Attachids** and **ParentID** fields to note the relationship between e-mail messages and their attachments. The example in Figure 10 shows attachments that are e-mail messages themselves, but attachments can also be electronic documents, such as a spreadsheet.



Producing eDiscovery

Up to this point, this document has discussed how to process, load, search, and review eDiscovery. This section explains how to produce eDiscovery in response to opposing counsel's request for production of documents. Four topics are covered:

- Using Summation to produce eDiscovery
- Using Summation to create a production **Briefcase** (for Summation iBlaze systems only)
- Using Summation to create a production **Browser Briefcase** (for Summation iBlaze systems only)
- Using a service bureau to produce eDiscovery

With Summation, you can produce eDiscovery in four different formats:

- In the documents' native formats, or as close to them as was made available to you
- In a generic electronic format, such as a text file or a file in HTML format
- As petrified images delivered in electronic form (such as PDF or TIFF files)
- As petrified images delivered in paper form

There is no particular right format to use for all occasions. Consider the following factors when you determine the format or formats to use for production:

- Requirements imposed by statute, rules, regulations, and case law
- The dictates of any applicable court orders
- Approaches mandated by governmental organizations such as the Justice Department and the Federal Trade Commission
- Opposing counsel's production request or preferences
- The ways in which you intend to use the eDiscovery during the course of the litigation
- Redaction requirements
- Usability of eDiscovery produced in the various formats
- Costs associated with producing eDiscovery in the various formats
- Agreement of the parties

In the example used throughout this document, opposing counsel has requested all paper and electronic documents related to the phrase **flat space** or the word **flood**. Opposing counsel has demanded that eDiscovery (electronic documents, e-mail, and e-mail attachments) be produced in its native format.

Using Summation to Produce eDiscovery

This section explains how to use Summation's **Production Tools** to create a **Briefcase** of electronic and scanned responsive documents. This process generates a set of documents and a related index that can be copied to CD-ROM and sent to opposing counsel. You can learn more about the **Production Tools** from the *Summation Production Tools (Or Taking Pain Out Of Document Productions)* white paper on the Summation web site: <http://www.summation.com/papers/>.



Note: To produce e-mail messages in .PST or .MSG format, you must first process the messages with the **eDiscovery Console**. If you do not do this, Summation will not be able to locate the original e-mail messages to copy to the **Briefcase**. For more information, see the Processing eDiscovery section of this document.

The procedure outlined in this section assumes that you have completed your document review and have the column view open with the summaries associated with the document you want to produce.

Note: This is your opportunity to petrify and redact the privileged electronic discovery (for more information, see the Producing eDiscovery as Petrified Images appendix to this white paper). Electronic documents containing privileged information must be petrified before they can be redacted. You must petrify the necessary electronic documents before you renumber your production set, to ensure the correct number of pages is captured for the image version of the documents (for example, a petrified Microsoft Excel spreadsheet may consist of 10 pages, whereas the original electronic version would be considered a one-page document).

To produce eDiscovery (in this example, e-mail messages in .MSG format, which opposing counsel can view with Microsoft Outlook):

1. With the column view in focus, from the **Summary** menu, select **Production Tools** and **Make a Production Set**.
The **Make a Production Set** dialog box is displayed.
2. Click **Set Production Numbers**.
If you have previously numbered a production set, a dialog box is displayed asking whether you want to clear out the old production numbers.
3. Click **Yes**. (If you do not want to clear out old production numbers and only want to number newly added documents, click **No** to maintain any pre-existing Bates numbers. For the purpose of this example, click **Yes** because a completely new production set is being created.)
A dialog box is displayed asking whether you want to clear production number data (**Prodno**) before renumbering.
4. Click **Yes**.
If any database summaries include a blank **Page Count** field, Summation prompts you to verify the page count field based on the image files associated with each summary.

*NOTE: An incorrect or blank page count value may adversely affect your production numbering. We recommend you select **Yes** to verify the **Page Count** field value, if you are not sure whether the **Page Count** field is accurate.*

5. Click **Yes**.
A prompt is displayed asking whether you want to verify that the image files associated with all selected database summaries exist.

*NOTE: A missing image file may adversely affect your production set. Summation recommends that you click **Yes** to verify that image files exist, if you are not sure whether all image files exist in the location indicated in the **ImgInfo** table.*



6. Click **Yes**.
When image file verification is complete, Summation checks for duplicate summaries (based on the **ImgTag** in the **ImgInfo** table) and displays a warning message, and also writes the errors to a log that you can view in any text viewer (the log file is stored in the following location: X:\iBlaze25\CaseData\ - 7. Click **Yes** to view the log file.
The log file is displayed in your default text viewer.
 - 8. Close the log file when you are finished reviewing it.
The **Renumber Documents for a Document Production Set** dialog box is displayed.
 - 9. In the **Beginning Production Document Number** box, type the beginning production document number (Bates number) for the production set.
 - 10. Click the column view to bring it into focus.
The column view is displayed forward from the **Renumber Documents for a Document Production Set** dialog.
 - 11. Review the production set for privileged or non-relevant documents. These documents should not be included in your production set. Conduct this review before you number your production.
 - 12. Click the field number for each summary that is associated with privileged or non-relevant documents. These documents should be marked before you number your production set to avoid creating gaps in it. You can mark multiple summaries by using holding your **Ctrl** key to mark non-sequential summaries or your **Shift** key to mark sequential summaries. (To unmark a summary, click its field number. To unmark all summaries, right-click the field number of any summary and select **UnMark All**.)
The color of each marked summary changes from white to aqua. Unmarked summaries will be numbered and included in the production set, and marked summaries will not be numbered and will be excluded from the production set.
 - 13. Click the **Renumber Documents for a Document Production Set** dialog box to bring it back into focus, and click **Renumber Documents**.
A prompt is displayed, informing you of the number of records that were added before numbering. These records are either attachments that were not previously included, or the parent record of an attachment.
- NOTE: The set of documents identified for renumbering may include only a portion of a compound document (for example, an e-mail message without its attachment(s)). In this instance, the Summation **Production Tools** automatically retrieve all summaries associated with the included family member(s). If the document has one or more attachments, the attachment summaries are retrieved and marked in cyan; if the document is an attachment to another document, the parent summary and all other sibling summaries (if any) are retrieved and marked in cyan. (For more information about compound documents, see the Producing Compound Documents in Summation appendix to this white paper.)*
14. Click **OK**.
A prompt is displayed, informing you of the number of documents and pages that were numbered.



15. Click **OK**.
The **Renumber Documents for a Document Production Set** dialog box is redisplayed. If you want to continue adding documents to the production set, you can search the database and apply Bates numbers to additional documents. For the purposes of the example in this white paper, all relevant documents have been numbered.
16. Click **Return to 'Make Production Set'**.
The **Make a Production Set** dialog box is displayed.
17. Click **Review Production Set** to quickly review the production set to verify that only the relevant documents were added.
The **Review Production Set** dialog box is displayed, with the column view in the background.

*NOTE: If you built your production set from a sequence of queries, you should review the aggregate set as a matter of due diligence. The review process aggregates the various query sets and subsets into a single columnar report containing the production Bates numbers in the **ProdNo** field. (If you do not have the **Prodno** field displayed in your column view, you can add it by clicking the **Fields** heading and dragging **Prodno** to the location in the column where you want it to be.)*

18. Click **Modify Production Set** to review the documents as a matter of due diligence.
The column view and the **Renumber Documents for a Document Production Set** dialog box are displayed. Before proceeding to printing or creating a production **Briefcase**, you must redact privileged information on the documents.

*NOTE: If privileged electronic evidence is contained in your production, click **Set Production Format** on the **Review Production Set** dialog box. See the Producing eDiscovery as Petrified Images appendix to this white paper.*

19. In the **Case Tools** area, click **Image Viewer**.
The **Image Viewer** is displayed.
20. From the **Options** menu, select **Markup Mode** and **Edit Markups**.
A toolbar is displayed on the **Image Viewer** window.
21. Browse through the production set and locate the documents that need redacting.
22. Select the **Redact** tool (the third icon from the right on the toolbar).
Your cursor is displayed as crosshairs.
23. Select the area on the image that you want to redact by dragging your cursor over it.
The area is redacted. To change the color of the redaction or add text to it, right-click the redaction and select **Properties**. Use the **Properties** options to customize your redaction as needed.
24. If everything is the way you want it, click **Return to 'Make Production Set'**.
The **Make a Production Set** dialog box is redisplayed.



25. Enter information about the production set in the **Production Set Info** area as follows:
- In the **Title** field, type a title for the production set. For this example, type the following:

Responding Documents, Set 1
 - In the **Date** field, type the date on which the documents are to be produced.
 - In the **Description** field, type additional information to help you easily identify the production set in the future.
26. Click **Make Production Set**.
If you are a Summation iBlaze user, a prompt is displayed asking if you want to **Briefcase** the documents as a production set. Click **Yes** and proceed to the next section.

Creating a Production Briefcase (Summation iBlaze edition only)

Summation iBlaze users can create a production **Briefcase**, which packages together discovery documents (paper and electronic) with an index of related database summaries.

This section continues where the last Step in the *Using Summation to Produce eDiscovery* section left off, assuming that you clicked **Yes** when prompted to **Briefcase** the documents as a production set (Figure 11).

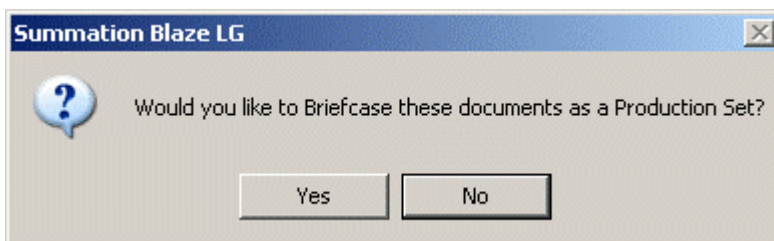


Figure 11: Briefcase Documents as a Production Set Dialog Box

After you click **Yes**, the **Choose Columns for Briefcase** dialog box is displayed.

1. Specify the columns that you want to include in the summaries that will be included with the **Briefcase**. To add columns, click the **Fields** heading on the column view and drag the fields that you want to add to the location where you want them placed. To remove columns from the view, drag the column heading to the blue title bar.

*NOTE: If you are providing this production to opposing counsel, you probably do not want to include coded data. Moreover, if you have provided new Production IDs that are different from your Beginning Document Numbers (Bates numbers), you should be sure to list the **Prodno** field and not the **DocID** or **BegDoc#** field.*

2. Click **OK**.
The **Specify Briefcase Purpose** dialog box is displayed.



3. Select **iBlaze use and review** and click **OK**.
The **Production Briefcase Image Markups** dialog box is displayed.
4. Select the markup options that you want to apply to the production documents in your production set. You can choose from the following options:
 - **Do not copy image markups** – Image markups are not copied to the documents in the production set.
 - **Burn-In** – Redactions, stamps, and the production document set label are burned in to the documents in the production set, as specified.

There are three ways to set a document label:

- Use a predefined label – By default, the **Doc Label** box contains the predefined value (if one is set) from the **Document Label** tab of the **Multi-Stamp Setup** dialog box. (For more information about the **Multi-Stamp Setup** dialog box, see the online Help in Summation.)
 - Display a label showing the contents of a field – Set a field value on the **Document Label** tab of the **Multi-Stamp Setup** dialog box and copy and paste that value in the **Doc Label** box. Note that you must copy and paste a field value; it will not be auto-filled.
 - Type custom text – You can type a label in the Doc Label box and your text will supercede a predefined label or field value, if one is set.
5. Click **OK**.
The **Briefcase Documents' Electronic Versions** dialog box is displayed. This dialog box allows you to select the default formats to use for the production of e-mail messages, e-mail attachments, and electronic documents. The formats you choose are included in the **Briefcase**, unless a value appears in the **ProdAs** field for a specific summary. If there is a value in the **ProdAs** field, it overrides the default setting. (For more information, see the *Producing eDiscovery as Petrified Images* appendix.)
 6. Select the eDiscovery production formats that you want to use for the production of e-mail messages, e-mail attachments, and electronic documents. You can select from the following options:

*NOTE: If you select a default option (native or petrified) and that item does not exist, an error log is generated that identifies summaries where eDiscovery documents were not copied to the **Briefcase**.*

- **eMail default format... Native** – E-mail messages are packaged in their native formats, or as close to their native formats as Summation allows. In the **Package non-Petrified eMails within...** area, you can opt to package e-mail messages in the following ways:
 - .MSG files using Microsoft Outlook – each e-mail message is included with an associated summary in the same production **Briefcase** as produced electronic documents and images
 - .PST files using Microsoft Outlook – e-mail messages are bundled into a .PST file that is separate from the other documents being produced
 - HTML files – each e-mail message is saved in HTML format using the Bates number as the file name, and is included with an associated summary in the production **Briefcase**



NOTE: In iBlaze Version 2.5.2 and previous, e-mail messages received in .NSF format can be produced in HTML format only.

- **eMail default format... Petrified** – The image (or petrified) format of each e-mail message is included with an associated document summary in the production **Briefcase**. This is designed for use only with a small number of summaries.
- **eMail Attachment default format... Native** – The native electronic version of each e-mail attachment is included with an associated summary in the production **Briefcase**.
- **eMail Attachment default format... Petrified (Image version)** – The image (or petrified) version of each e-mail attachment is included with an associated document summary in the production **Briefcase**. This is designed for use only with a small number of summaries.
- **eDoc default format... Native** – The native electronic version of each document along included with an associated summary in the production **Briefcase**.
- **eDoc default format... Petrified (Image version)** – The image (or petrified) version of each document is included with an associated document summary in the production **Briefcase**. This is designed for use only with a small number of summaries.
- **Briefcase OCR Text (not recommended)** – OCR text is included in the production **Briefcase**. This option is not recommended because if an image is redacted and the OCR text is included in the **Briefcase**, the privileged text underlying the redactions will be disclosed in the OCR text.
- **Document set is DocID sorted (recommended)** – If the database summaries are sorted by the **DocID** field, use this option. This option is recommended because it accelerates the creation of the **Briefcase** by making use of the fact that the summaries are sorted.
- **Log absence of Petrified version as an error** - This option is available only if you choose to save one type of eDiscovery as petrified documents. The option writes the instances when a petrified format of an eDiscovery document does not exist in a log file, even though you selected to produce the document in that format.

For the example used in this white paper, you need to produce eDiscovery in native formats. Select the options **eMail default format... Native, Package non-Petrified eMails within... Native, eMail Attachment default format... Native**, and **eDoc default format... Native**. Also select the **Document set is DocID sorted** option, but make sure that your summaries are sorted by the **DocID** field before continuing.

7. Click **OK**.

Summation saves the images and adds them to the **Briefcase**. Status bars are displayed so that you can monitor the progress. When the **Briefcase** is complete, it is added to the **Case Explorer** under **Document Collections** with a production **Briefcase** icon (Figure 12).

*NOTE: **Briefcase** files are stored in the following location:*

X:\iBlaze26\CaseData\\Profiles\All Users\SRS

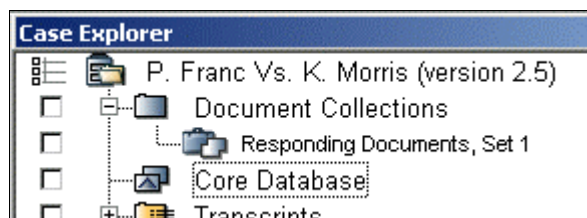


Figure 12: The Responding Documents, Set 1 Briefcase

Creating a Production Browser Briefcase (Summation iBlaze edition only)

If opposing counsel does not have Summation, you can use the Summation iBlaze Browser Briefcase to send your production. The Browser Briefcase bundles a copy of the index (the Briefcased summaries) in HTML format with copies of the corresponding discovery documents (images, e-mail messages, e-mail attachments, and electronic documents).

To create a **Browser Briefcase**:

1. In the **Case Explorer** under **Document Collections**, double-click the **Briefcase** for which you want to create a **Browser Briefcase**. (For the example used in this white paper, double-click **Responding Documents, Set 1**). The **Briefcase** is opened.
2. Click the **Briefcase** to bring it into focus.
3. From the **Options** menu, select **Export Data & Images to Browser Briefcase**. A dialog box is displayed, asking whether you want to export associated images to PDF format instead of the default multi-page TIFF format.
4. Click **Yes** for the purposes of this example. The **Browse for Folder** dialog box is displayed.
5. Browse to and select the location where you want to store the **Browser Briefcase**, and click **OK**. (If you want to save the **Browser Briefcase** to a new folder, create the folder before starting this procedure.) A prompt is displayed, confirming the location you specified.
6. Click **OK**. A status message is displayed on the bottom of your Summation screen. When the **Browser Briefcase** is created, a prompt is displayed allowing you to view the **Browser Briefcase**.
7. Click **Yes**. Your browser opens and displays the **Browser Briefcase**.

*NOTE: To view the documents and images, click the icons in the **Linked Doc** column. Adobe Acrobat is used to open saved in PDF files, or the available standard image viewer is used for images saved in .TIFF format. Electronic documents are displayed in their native applications or in the preferred image viewer on your computer.*



Using a Service Bureau to Produce eDiscovery

You can work with your service bureau to have them produce, on your behalf, eDiscovery that is loaded in your Summation system. Service bureaus produce eDiscovery on various ways. Consult your service bureau to determine the best method for both of you.



Appendices



Appendix 1: Glossary of Terms

The terms in this glossary and used throughout this white paper are intended to give you a better understanding of how to use Summation effectively for eDiscovery. They are not intended to have any legal significance.

Terms

Term	Definition
Authenticating volume	Some form of storage medium obtained from a client or opposing party that contains electronic information in native file formats. It may be the original medium or a copy provided during discovery, which allows one to trace electronic files back to a source that can be authenticated.
Blaze	Summation's technology for faster searching and sorting. Blazing can increase search speeds by orders of magnitude over traditional searches. When you Blaze a database or transcript, a complete vocabulary list is generated. <i>Note: When you Blaze transcripts, the noise words are not included in the vocabulary list. Use Summation utilities to Blaze your database or transcripts.</i>
Briefcasing	The process by which database records and images are copied for reference while offline. You can access Briefcased records and images form the Document Collections folder in the Case Explorer .
child document	A document that is attached to another document (for example, a file that is attached to an e-mail message).
compound document	All of the documents included in a parent/child relationship of documents (for example, an e-mail message and its attachments comprise a compound document).
DII file	The Document Image Information (DII) file is a text file that is used to load a large number of images into Summation's ImgInfo table.
document format	The format in which the document's data is stored (for example, a Microsoft Word file).
eDiscovery	Electronic discovery (eDiscovery) is the process of identifying, gathering, processing, and working with the electronic files of parties to a lawsuit. An extension of paper-based discovery, it shares many of the same characteristics but presents challenges of its own. The term eDiscovery can also refer to the electronic files themselves.
eDocs	The Summation electronic document handler.
electronic evidence	Writings that are created, exchanged, or archived electronically. Electronic evidence includes any file that is saved electronically, such as Microsoft Word documents or Microsoft Excel spreadsheets, e-mail messages, digital audio or video files, digital photographs, program code, database records, and so forth.
electronic exhibit	Electronic files used as an exhibit at a deposition.
eMail	The Summation e-mail handler.



Term	Definition
focus	The window in Summation that is currently active and upon which you can carry out commands is in focus. When a field is in focus, it is highlighted. An item in focus has a different appearance than all other similar items.
metadata	A widely-used and seldom-defined term in eDiscovery circles, metadata is structured information about an electronic file that generally is not intentionally inserted by, and often never noticed by, the creator or users of that file. A simple way of viewing metadata for an electronic document such as a Microsoft Word file is to select Properties from the File menu on the top menu bar in Microsoft Word. The dialog that displays shows examples of metadata associated with the file.
.MSG	The file name extension used by Microsoft Outlook for e-mail messages.
.NSF	The file name extension used by IBM for many of its Lotus Notes and Domino applications. Lotus Notes electronic mail and similar items are stored in .NSF files.
ocrBase	The Summation module that permits the loading and searching of full-text versions of imaged documents. The ocrBase is available in the Summation Gold and iBlaze editions.
package	A collection of volumes or storage media such as CDs, DVDs, hard drives, and so forth.
parent document	A document that has an attachment (for example, an e-mail message that has a file attached to it).
PDF file	Files in Portable Document Format (PDF) are portable across computer platforms and operating systems. They can be viewed with Adobe Acrobat.
petrification	The process used to save an electronic document or e-mail message as an electronic image. For example, a Microsoft Word document can be petrified by saving it as a series of images in TIFF format. Petrification can be used when it is necessary to redact portions of a document. Rather than print a document, redact portions, scan the document, and then load it back into Summation, you can petrify it and redact the appropriate portions on the saved image file.
production set	The set of documents that you produce to opposing counsel.
.PST file	The file name extension for the data file Microsoft uses to save Outlook messages, tasks, appointments, and journal entries.
storage media	Physical object on which electronic information is stored. Media includes, but is not limited to, CDs, DVDs, floppy diskettes, hard drives, optical disks, tape cartridges, USB memory devices, and Zip drives. They can also include cellular phones, facsimile machines, personal digital assistants (PDAs), and printers – anything, in short, capable of holding electronic information for extended periods of time.
store format	The format in which a collection of documents are stored (for example in a Zip file).
TIFF	Tagged Image File Format is a common format for scanned documents.



<i>Term</i>	<i>Definition</i>
volume	A single piece of storage media from a package – CD, DVD, hard drive, and so on – that may contain one or more electronic files.



Appendix 2: Electronic File Formats Supported by Summation's Native Indexer

Summation's native indexer is capable of processing the following electronic file formats:

- Adobe Acrobat (.pdf), All versions through Version 6
- ANSI text
- Corel WordPerfect (.wp and .wpd), Versions 5.0 through WordPerfect 2002
- HTML (.htm and .html)
- Microsoft Excel (.xls and all variations)
- Microsoft Outlook Express message stores (*.dbx), Versions 5 and 6
- Microsoft PowerPoint 97, 2000, and XP (.ppt)
- Microsoft Word (.doc and all variations), Word for DOS and all Windows Versions through Microsoft Word XP
- Microsoft Works
- Rich Text Format (.rtf)
- Standard text (.txt)
- Unicode
- Write
- XML (.xml)
- All of the above in Zip files

Note: Files contained in Zip files are indexed and searchable. Summation displays an excerpt on the **Search Results** page when a **Case Explorer** search is executed, but the file name displayed is the name of the Zip file. Furthermore, the **eDocs Viewer** does not display the text of the document(s) contained in the .zip file, but only displays a message that reads: "This eDoc is a ZIP file."

Quick View Plus or other text extraction software can be used to save unsupported file formats as file formats that Summation can index.

Note: It is important to be aware of files that are password-protected or encrypted. You can load and view encrypted PDF files, but Summation cannot index and search the text in these files. In addition, Summation cannot index Microsoft Word files that were password-protected for opening. However, Summation can index and search Microsoft Word files that were password-protected for modification.



Appendix 3: The eDiscovery Console

The **Process Entire Volume** option was used in the main body of this document to illustrate how you can handle entire volumes of eDiscovery quickly and efficiently. This appendix covers two main topics:

- *Processing Selected .PST or .NSF Files* – Explains how to processing selected .PST and/or .NSF files, as opposed to an entire volume
- *Using the View or Modify Mail Files Tab* – Explains how to process .PST or .NSF files that were loaded into Summation, but that were not previously processed

Processing Selected .PST or .NSF Files

The **Process Select Mail Files** tab of the **eDiscovery Console** allows you to pick specific .PST or .NSF files to process. For example, you might want to load select .PST or .NSF files from different folders on one volume.

To process selected .PST or .NSF files:

1. With the **Core Database** in focus, select **Process eDiscovery** from the **File** menu.
The **eDiscovery Console** is displayed.
2. Click the **Process Select Mail Files** tab.
The **Process Select Mail Files** tab is displayed topmost (Figure 13).

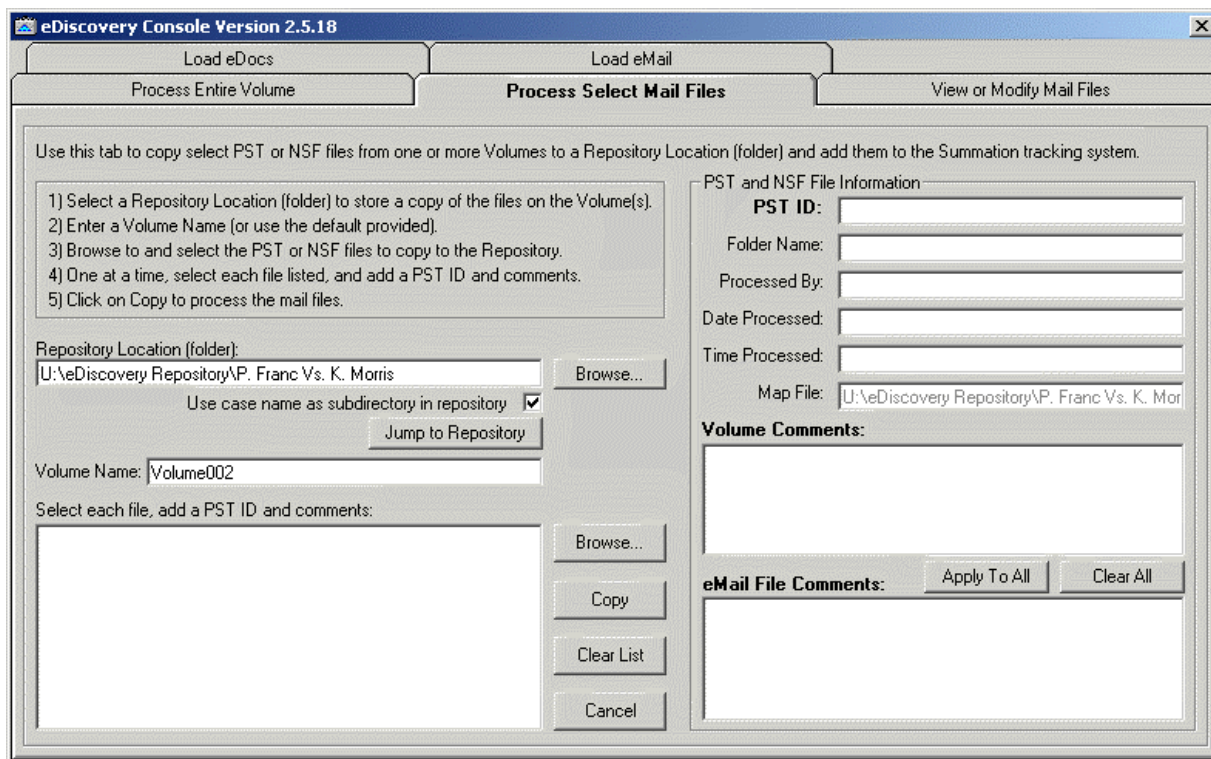


Figure 13: eDiscovery Console, Process Select Mail Files Tab



3. Click **Browse** next to the **Repository Location (folder)** and select a folder to store your .PST and .NSF files.
4. Click **Browse** next to the **Search each file, add a PST ID and comments** area. The **Select Mail Files** dialog is displayed.
5. Browse to and select the .PST and/or .NSF files that you want to process, and click **Open**.
The files are listed in the **Search each file, add a PST ID and comments** area. Repeat this step until you have selected all the .PST and/or .NSF files that you need.
6. Click each file to view and/or change its PST ID in the **PST ID** field.
7. Enter a name for the volume in the **Volume Name** box, or use the provided default name.
8. Enter any comments about the volume in the **Volume Comments** box.
9. To add comments to a .PST or .NSF file, click the file and type your comments in the **eMail File Comments** box. Click the **Apply this comment to all PST files** check box if you want your comments to apply to all the files.
10. Click **Copy** to copy the .PST and/or .NSF files.
The files are copied to the repository selected in the **Repository Location (folder)** box. They are also added to Summation, as was done in the *Processing eDiscovery* section of this white paper.

Using the View or Modify Mail Files Tab

The **View or Modify Mail Files** tab of the **eDiscovery Console** allows you to process .PST and .NSF files that were loaded into a Summation, but were not previously processed (for example, if a DII file was used to load the eDiscovery prior to Version 2.5). You will need to use this tab if you want to produce evidence from these files.

The .PST and/or .NSF files are not copied to the repository where your other eDiscovery is stored, but rather remain in their original locations.

To process .PST and/or .NSF files that were previously loaded, but were not processed:

1. With the **Core Database** in focus, select **Process eDiscovery** from the **File** menu.
The **eDiscovery Console** is displayed.
2. Click the **Process Select Mail Files** tab.
The **View or Modify Mail Files** tab is displayed topmost (Figure 14).

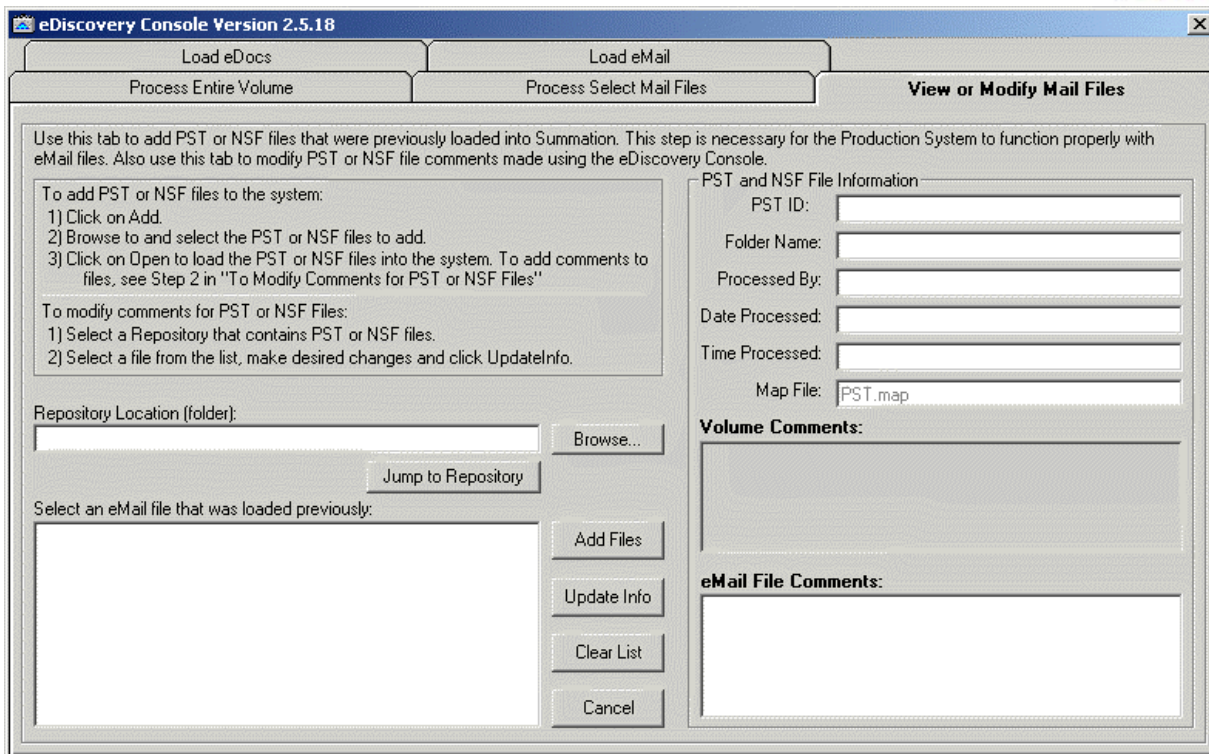


Figure 14: eDiscovery Console, View or Modify Mail Files Tab

3. Click **Add Files**.
The **Select Mail Files** dialog box is displayed.
4. Browse to and select the .PST files that were previously loaded into a Summation case, but were not processed by the **eDiscovery Console**. Click **Open**.
The files are listed in the **Select an eMail file that was loaded previously** area.
5. Modify the **PST ID** and **eMail File Comments** as needed. (The other **PST and NSF File Information** fields are read-only on this tab.)
6. Click **Update Info**.
The files are processed.



Appendix 4: eDiscovery/Service Bureau Fields

The Summation E-table, created automatically for all new cases, is designed specifically to better store and track eDiscovery. Below is a table that lists the eDiscovery specific fields in the E-table with a brief description of the data that populates the field.

Note: *This list is simply a starting point and can be expanded. You can customize your table to accommodate extraction of additional types of metadata to load into the Summation **Core Database**. At that point, you can load the additional data or have a service bureau load the data into the custom table. You may want to give a copy of this information to the service bureau that is processing eDiscovery for you, so the bureau is aware of the metadata that you expect them to extract.*

E-Table Fields

E-Table Field	Description	Used For
Applicat	Application	eMail
Attrange	Attachment IDs	eMail
Atttitle	Attachment Title	eMail
Author	Author (same as From in an e-mail message)	eMail
Bcc	BCC	eMail
Body	Body	eMail
Cc	CC	eMail
Datecrtd	Date Created	eMail
Datercvd	Date Received	eMail
Datesent	Date Sent	eMail
Datesvd	Date Last Saved	eMail
Docid	Document ID	eDocs and eMail
Doclink	Attachment Location	eMail
Doclink	Path and file name of document	eDocs
Folder	Folder Name	eMail
Folderid	Folder ID	eMail
From	From	eMail
Header	Header	eMail
IntMsgID	Internet Message ID	eMail
Media	Media	eDocs and eMail
Msgid	Message ID	eMail



<i>E-Table Field</i>	<i>Description</i>	<i>Used For</i>
Numattch	Attachment Count	eMail
Parentid	Parent ID	eMail
Read	Read/Unread	eMail
Storeid	Store ID	eMail
Subject	Subject	eMail
Timercvd	Time Received	eMail
Timesent	Time Sent	eMail
To	To	eMail



Appendix 5: DII Tokens for Loading Electronic Documents or E-mail Messages

To accommodate loading eDiscovery processed by service bureaus, Summation has extended the DII file format used in Summation versions prior to Version 2.5. The extended DII file includes all tokens and formats from the standard DII file, as well as the following additional tokens.

DII Tokens for Loading Electronic Documents and E-mail Messages

Token	Field Populated	Description
@APPLICATION	APPLICAT	The application used to view the electronic document. For example: @APPLICATION Word
@ATTACH	ATTCHIDS <multi-entry> (Field selected for related attachment Doc IDs in Link Fields defaults)	IDs of attached documents. Appending the value allows the DII to populate multiple values in the ATTCHIDS field. For example: @ATTACH EML0001; EML0002
@ATTACHRANGE	ATTRANGE	The document number range of all attachments if more than one attachment exists. Each attachment, along with the e-mail message, will be loaded into Summation as its own record. The attachment range would be populated with the document number of the first attachment and the last number of the last attachment. For example: @ATTACHRANGE WGH000008 – WGH000010
@ATTMSG	N/A	Relative or full path and file name of the e-mail attachment that is an e-mail message itself. The file will be copied to the MSF folder . The Media field will be populated with the term eMail and the FOLDERID field is coded with the session name assigned during the load of DII.
@BATESBEG	BATESRNG	Beginning Bates number, used with @BATESEND . For example: @BATESBEG SGD00001
@BATESEND	BATESRNG	Ending Bates number, used with @BATESBEG . For example: @BATESEND SGD00055
@BCC	BCC	Anyone sent a blind copy on an e-mail message. For example: @BCC Nick Thomas



Token	Field Populated	Description
@C		<p>Optional code used to load data into specified fields in the user's document database. This helps decrease the amount of data entry required for the database users. It is meant for use when the same value is repeated for a group of documents, such as documents that all have the same box number or author. The syntax of using the @C token is:</p> <p>@C <FIELDNAME> <DATA></p> <p>For example, to fill in the ISSUES field of the database with the value Mental Health, the line would read:</p> <p>@C ISSUES Mental Health</p> <p>For consecutive DII records where these values are the same, you do not need to repeat the @C line. Instead, insert the next @C line in the next DII record where the data changes. To stop entering data in a field, insert an @C line with the field name following by nothing.</p>
@CC	CC	<p>Anyone copied on an e-mail message. For example:</p> <p>@CC John Ace</p>
@D	DEFDIR	<p>Required token for each DII record that has an image associated with it and designates the directory location of the image file(s). The data specified after the @D goes into the Default Directory (DEFDIR) field of the ImgInfo table. There are three different ways to denote the DEFDIR:</p> <ol style="list-style-type: none"> 1. @I (to refer to the Case Customize Image Location) 2. The hard coded drive letter and path into the DEFDIR field 3. @V (to refer to the specified volume label of the CD-ROM) <p>For example:</p> <p>@D @V CD-101:\Box_34</p> <p>Note: Users of Summation iBlaze/LG can use UNC paths after the @D to specify a folder containing images.</p>
@DATECREATED	DATECRTD	<p>The date that the file was created, if applicable. For example:</p> <p>@ DATECREATED 01/04/2003</p>
@DATERCVD	DATERCVD	<p>Date that the file was received. For example:</p> <p>@DATERCVD 01/04/2003</p>
@DATESENT	DATESENT	<p>Date that the file was sent. For example:</p> <p>@DATESENT 01/04/2003</p>
@DATESAVED	DATESVD	<p>When the file was saved, if applicable. For example:</p> <p>@ DATESAVED 01/04/2003</p>
@DOCID	DOCID <note>	<p>Document ID of a full-text document, e-mail message, or electronic document. If the DII includes full-text files, then the DOCID value (instead of the @T value) is used to load and associate ocrBase documents with the appropriate summary. For example:</p> <p>@DOCID EML00017</p>



Token	Field Populated	Description
@EATTACH	DOCLINK <note> (Field selected for Linked Documents in Link Fields defaults.)	Relative or full path and file name of the attachment. The file will be copied to the eMail directory and the relative path of the file will be placed in the DOCLINK field. The MEDIA field will be populated with the term Attachment . For example: @EATTACH\\Server\Files\Flood Damages.xls
@EDOC	DOCLINK	Relative or full path and file name of the electronic document. The file will be copied into the eFiles directory and the relative path of the file will be placed in the DOCLINK field. The MEDIA field will be populated with the term eDoc . For example: @EDOC D:\eDoc\WordDoc.doc
@EDOCIDSEP	DOCID	This token is intended for service bureaus that use their own tracking numbers (for example, TRACK001_Doc001.txt). This token allows Summation to remove the tracking ID (TRACK001) from the file so that it can be replaced with a Summation naming convention. The token uses a one-character string a value to indicate the demarcation in the file name. In the example above, the underscore character separates the tracking number from the file name, so the token should be followed by the underscore character. Use this character at the top of the DII file above the individual records. For example: @EDOCIDSEP _
@EMAIL-BODY	BODY <note>	Body of an e-mail message. Must be a string of text contained between @EMAIL-BODY and @EMAIL-END . The @EMAIL-END token must be on its own line. For example: @EMAIL-BODY <E-mail message text> @EMAIL-END
@FOLDERNAME	FOLDER	The name of the folder that the e-mail message came from. For example: @FOLDERNAME Conner-Stevens – Mailbox\CStevens\Inbox
@FROM	FROM	From field in an e-mail message. For example: @FROM Kelly Morris



Token	Field Populated	Description
@FULLTEXT		<p>Indicates that there are OCR documents attached to the record. The file names must match the names of the images (not including the extension), and they must be located in the same place.</p> <p>Variations:</p> <p>@FULLTEXT DOC - One full-text file exists for each database record.</p> <p>@FULLTEXT PAGE - One full-text file exists for each page of the document summary.</p> <p>These tokens should be placed before any @T tokens. Similar to the @C token, this statement remains in effect until turned off by using the opposite designation. In other words, if you are using the PAGE method, turn it off by using @FULLTEXT in the record that does not contain a full-text file.</p>
@FULLTEXTDIR		<p>The @FULLTEXTDIR token is a partner to the @FULLTEXT token. This token provides more flexibility to both the service bureau and the client when loading a DII file that includes full-text files. The @FULLTEXTDIR token allows the service bureau to specify a directory from which the full-text files will be copied during the load. Therefore, the full-text files do not have to be located in the same directory as the images at the time of load. The @FULLTEXTDIR token gives users the flexibility to load the DII file and full-text without requiring them to copy the full-text to the network first.</p> <p>An example of the syntax used with the @FULLTEXTDIR token is:</p> <p>@FULLTEXTDIR Vol001\Box001\ocrFiles</p> <p>The above example shows a relative path, which indicates to Summation that it should search for the full-text files in the same location as the DII file that is being loaded and follow any subdirectories in the @FULLTEXTDIR argument. The relative path works whether the DII file is on a network drive or on a CD as a sibling of the Vol001 folder.</p> <p>Just as @FULLTEXT PAGE and @FULLTEXT DOC apply to all subsequent records in the DII file until they are turned off (by adding the token after the last record that includes full-text), the @FULLTEXTDIR argument applies to all subsequent records in the DII file until it is changed or turned off (by including the token with a blank argument).</p>
@HEADER	HEADER <note>	<p>E-mail header content. The @HEADER-END token must be on its own line. For example:</p> <p>@HEADER <Header Text> @HEADER-END</p>
@I	DEFDIR	<p>This token is used with the @D token. The @I token refers to the image location specified in Case Customize. This location must be a drive letter (or UNC path for iBlaze/LG users) and path that points to the directory where the images are stored. Summation users can select any valid location or use Summation's default location, the IMAGES subdirectory under the Case Directory. In either case, the image files must be copied to this location.</p>



Token	Field Populated	Description
@INTMSGID	INTMSGID	Internet message ID. For example: @INTMSGID <00180c34fe5\$bf2d54b0\$0500000a@SKEETER>
@L	LONGNAME	This token is optional code and denotes the long name or description of the image file(s). The data after @L goes into the LONGNAME field of the ImgInfo table. <i>Note: This applies to Summation Blaze Version 5.21 and earlier, and is used in the IMGINGO table.</i> For example: @L Patient History Form
@MEDIA	MEDIA	Populates the Media field with the designated value (for example, eDoc , eMail or Attachment). If the value indicated in the token differs from the Summation default, or an entry exists in the field, then the most recent process wins and an entry is made in the error log. Because of this, use this token with care and only if you have a compelling reason. For example: @MEDIA eDoc
@MSGID	MSGID	E-mail message ID generated by Microsoft Outlook or Lotus Notes. For example: @MSGID 00000000E8324B3A0A800F4E954B8AB427196A1304012000
@MULTILINE	Any <note> field specified	Allows carriage returns and multiple lines of text to populate the specified <note> field. Text must be between @MULTILINE and @MULTILINE-END . The @MULTILINE-END token must be on its own line. For example: @MULTILINE NOTEFIELD Here is the first line. Here is the second line. Here is the last line. @MULTILINE-END For consecutive DII records where these values are the same, you do not need to repeat the @MULTILINE line. Instead, insert the next @MULTILINE line in the next DII record where the data changes. To stop entering data in a field, insert an @MULTILINE line with the field name following by nothing
@NOPAGECOUNT	DOCID	Turns off automatically using a number after a space in the Document ID as the number of pages. Allows Document IDs to contain spaces. Must be entered at the beginning of the DII file and applies to all records for the entire DII file. @NOPAGECOUNT @FULLTEXT page @TGHSPILT 3602 Q00555 @D @I Box011\Dir01\GHSPILT 3602 Q00555.tif



Token	Field Populated	Description
@O		<p>There are two uses for the @O token. This token is used when the full-text documents are located someplace other than the image location as specified by the @D line of the DII file. It tells Summation that there are full-text documents at this location. It is placed immediately below the @D line. There can be only one text file for the record, and it must have the name of the 1st TIFF image with a .TXT extension. The full or relative path to the full-text document must be included. For example:</p> <p>@O J:\docs\scanned</p> <p>The @O token can also be used to point to a .TXT file that does not have the same name as the TIFF file. It can be used when there are no TIFF files and it is the only way to load OCR from separate .TXT files when loading a Class II DII file.</p>
@OCR @OCR-END		<p>Some service bureaus and clients prefer a different approach to loading full-text than the traditional Summation method of requiring the full-text to be loaded from separate ASCII text files. Some clients prefer including the full-text in the DII file itself. The @OCR and @OCR-END tokens give service bureaus the flexibility to include the full-text (including carriage returns) in the DII file. This method of loading full-text significantly improves the speed of the DII load, by eliminating the need for the system to search for and locate each text file and open it to copy the text into the ocrBase.</p> <p>The @OCR-END token must appear on a separate line.</p> <p>Note: <i>When using the @OCR and @OCR-END tokens and including the full-text in the DII file, service bureaus cannot apply page breaks at specific locations in the full-text document.</i></p> <p>An example of the syntax used with the @OCR and @OCR-END tokens is:</p> <p>@OCR <full-text extracted from the electronic document, which can span multiple lines> @OCR-END</p>
@PARENTID	PARENTID <none> (Field selected for Parent ID in Link Fields defaults.)	Parent document ID of an attachment. For example: @PARENTID WGH000003



Token	Field Populated	Description
<p>@PSTCOMMENT</p> <p>@PSTCOMMENT- END</p>		<p>Users may want to record information about a .PST file that is loaded into a Summation case. For example, a user may want to identify where a specific .PST file came from and what it relates to (for example, client e-mail messages related to flat space and received on April 26, 2004). The comments are associated with the .PST file designated by the @PSTFILE token that follows. The comments can be viewed from the e-mail and attachment records generated from the .PST file designated in the @PSTFILE token.</p> <p>The @PSTCOMMENT token is used in conjunction with @PSTFILE. It should be followed by the @PSTCOMMENT-END token and must appear before the @PSTFILE token it applies to. The @PSTCOMMENT-END token must appear on its own line. For example:</p> <pre>@PSTCOMMENT <COMMENT TEXT> @PSTCOMMENT-END @PSTFILE EMAIL001\Pfranc.pst, Pfranc_04April_2004</pre> <p>Note: The comments will not be written to the Core Database record in Summation, but users can review the comments by right-clicking an e-mail record and selecting the Show PST Info option.</p>
<p>@PSTFILE</p>		<p>The @PSTFILE token is used to process the .PST file by designating: 1) the location of the .PST file at the time of load, and 2) the unique ID of the .PST file. The path to the .PST file can either be hard-coded or relative to the location of the DII file at the time of load. The unique ID should be the same value assigned by the user to the .PST file when processing using Summation's eDiscovery Console.</p> <p>If either necessary value is missing, the DII load will record an error and the .PST file that corresponds to the record with the missing information will not be processed.</p> <p>An example of the use of @PSTFILE:</p> <pre>@PSTFILE EMAIL001\Pfranc.pst, Pfranc_04April_2004</pre> <p>Summation gathers this information but does not process the .PST file until the DII load is complete. The PSTID (the second value) is populated into the PSTID field as designated on the eMail tab in the Defaults dialog box (accessed from the Options menu) in Summation. The PSTID argument assigned by the @PSTFILE token is assigned to the record it appears in and will apply to all subsequent e-mail records. The argument is applied until either the @PSTFILE token is turned off by setting it to a blank argument (such as: @PSTFILE), or the argument changes.</p> <p>The @PSTFILE token can occur multiple times in a single DII file and assign a different argument each time. This allows the service bureau to process multiple .PST files and present the data for all .PST files in a single DII file. For example, a service bureau can process five .PST files and include five instances of @PSTFILE tokens with five different arguments, all in the same DII file.</p>
<p>@READ</p>	<p>READ</p>	<p>Notes whether the e-mail message was read. For example:</p> <pre>@READ Y</pre>



Token	Field Populated	Description
@RELATED	OTHERIDS <multi-entry> (Field selected for Related Document IDs in Link Fields defaults.)	The document IDs of related documents. @RELATED WGH000006
@STOREID	STOREID <note>	The .PST identifier. Should not be used if @PSTFILE is used. For example: @STOREID
@SUBJECT	SUBJECT	The subject of an e-mail message. For example: @SUBJECT Town Issues
@T	IMGTAG	This token is required for each DII record and designates the ImageTag . It must be the first item listed for each database record. This data specified after the @T goes into both the Image Tag (IMGTAG) field in the ImgInfo table and the Column to Hold ImageTag in the Document Database . The image tags must be unique values. For this reason, many users choose the document number as the image tag. The image tags establish the link between the document database table and the ImgInfo table. When a user is in a document database record that has a corresponding image file and they want to view the image, Summation looks at the value in the Column to Hold Image Tag field in the database and reads the image file location from the ImgInfo table record with the matching value in the Image Tag field. For example: @T CR00293 1 Note: If there is a template on the Column to Hold Image Tag field of the user's document database, then the Image Tag must conform to the template format. For example, if the template forces the field to contain a certain number of digits, any image tag values that are comprised of fewer digits must be appropriately zero filled.
@TIMERCVD	TIMERCVD	Time that the e-mail message was received. For example: @TIMERCVD 11:00 a.m.
@TIMESENT	TIMESENT	Time that the e-mail message was sent. For example: @TIMESENT 10:59 a.m.
@TO	TO	To field in an e-mail message. For example: @TO Conner Stevens
@TRANS	DEPOIDS <multi-entry> (Field selected for Transcript Zoom in Link Fields defaults.)	The transcript description. The value populates the Transcript Zoom field. For example: @TRANS conner stevens v1.txt



Token	Field Populated	Description
@V		<p>This token is used with the @D token and refers to the volume label of the image location. By using a volume label instead of a drive letter, the user does not have to use the same drive letter designation for their media as had been used by the service bureau.</p> <p>The @V token is used most often with the images that are being burnt onto CD ROMs. Substitute the volume label for the drive letter in the @D line, still including the path leading up to and including the directory in which the images are located. The Summation user must set up the Drives Holding Images in the case Imaging Defaults so that Summation knows on which drive(s) to look for the specified volume(s).</p> <p>The volume label can be obtained from any drive by using the DIR command at the command prompt or by looking at the drive properties in Microsoft Windows Explorer/My Computer. When using the command prompt, the volume label will appear at the top of the directory display listing.</p> <p>Use the Map Volume to Directory option in imaging defaults if your images are on CD-ROM, you have used the @V (volume label) code in your DII file, and the volume label of the CD(s) is also the first subdirectory. Enabling this option tells Summation to map the volume label indicated after the @V in the DEFDIR line of the ImgInfo table to the drive letter(s) set in your Drives Holding Images:</p> <p>@Vol:=>A:\voll.</p> <p>Example:</p> <p>DEFDIR in ImgInfo Table: @VCD_00001:</p> <p>Drives Holding Images: D</p> <p>Maps to: D:\CD_00001\</p> <p>This option is commonly used when the CDs are stored on a Meridian tower, or when the volumes have been copied to a fixed drive from a CD ROM and the Volume labels are used in the manner described above.</p>

Note: Be sure to separate the token from the text that follows it with a space.

The **@T**, **@DOCID**, and **@EDOC** tokens are required in a DII file when loading electronic documents.

The **@T**, **@DOCID**, **@EMAIL-BODY**, **@EMAIL-END**, **@MSGID**, **@C**, and **@APPLICATION** tokens are required in a DII file when loading e-mail messages. If the e-mail messages have attachments, then the **@ATTACH**, **@PARENTID**, and **@EATTACH** tokens are also required.



Appendix 6: Producing eDiscovery as Petrified Images

One of the great strengths of Summation Version 2.5 and later is the capability to cost-efficiently work with eDiscovery in its native format. There are times, however, when you may need to use a paper paradigm, converting electronic documents or e-mail messages to image format, and extracting text for search and review. Typically, this requires using a service bureau or a large-batch eDiscovery package.

With Summation Version 2.5 and later, you have the option to *petrify* electronic documents, e-mail messages, and e-mail attachments. Petrification converts a file to image format (such as TIFF or PDF) and extracts information from it. The information is programmatically entered into a database summary.

This appendix explains how to petrify files and to create a production set comprised of the petrified files.

Note: *Judiciously converting to image format for redaction purposes is often wiser than attempting to redact information from a file in its native format. When you attempt to redact a file in its native format, you risk making undesired or unintended changes to the file.*

For example, suppose you have a Microsoft Word file that you need to produce in response to a set of requests for the production of documents, but that file also contains privileged information. You could open the file, delete the privileged information, and save the edits. However, when you open and modify the file and save the changes, you alter the file's metadata. The metadata might now identify you as the author of the document, list the date and time you saved the changes, and list the last date and time of the edit.

Reasons for producing eDiscovery in petrified form include:

- Portions of eDiscovery files need to be withheld from production for privilege or similar reasons, and redaction is the only viable means to accomplish this. Therefore, the files must be petrified.
- Opposing counsel has asked for eDiscovery in image format rather than native format.
- The parties have agreed, or the court has ordered, that eDiscovery will be produced as image files.

Summation's petrification tool is designed to meet the first reason, to convert a small number of electronic documents to image format in preparation for redaction. It is intended to petrify a maximum of 50 marked summaries at one time. If you need to convert a larger number of electronic documents to TIFF or PDF, consult a service bureau or consider using third-party software tools.

Petrification has the following requirements and restrictions:

- Petrification requires ePrint, QuickView Plus (for electronic documents), and Microsoft Outlook (for e-mail messages).
- Petrified versions of eDiscovery files do not include metadata. In addition, links to other files, formulas, and so on that were in the native files do not carry over to the image files.
- E-mail attachments are petrified in the same way as electronic documents or e-mail messages, depending whether the attachment is an electronic document or an e-mail message.



Petrifying eDiscovery

Petrify the eDiscovery documents that you need to redact before renumbering your production set. An eDiscovery document in native format is assigned a single Bates number at the file level, whereas a document in image format is assigned a Bates number for every page of the document. Therefore the number of pages in the resulting image file affects the accurate Bates numbering of the document.

You need to install the Summation **Petrification Toolset** in order to petrify your documents. Contact your Summation representative for additional information.

To petrify eDiscovery:

1. Click the field numbers of the summaries associated with the eDiscovery that you want to petrify.
The summaries are marked, and their rows are displayed in aqua.

NOTE: You can mark a maximum of 50 summaries for petrification.

2. From the **Summary** menu, select **Marking Options** and **Petrify Black and White Documents...**
The **Summation Electronic Document Petrification** dialog box is displayed, providing you with information about the petrification tool.

NOTE: Petrify black and white documents separately from your color documents. Petrified color documents display poorly on the screen, but print clearly.

3. Click **OK**.
An informational message is displayed, letting you know how many documents will be petrified.
4. Click **OK**.
The **Petrifying eDocs** dialog box is displayed, indicating the status of the petrification process.
5. Click **OK** when petrification is complete.
The electronic documents are now available for viewing in the **Image Viewer**.
6. Click the column view to bring it into focus, and, from the **Summary** menu, select **Tools** and **Verify Image Page Count**.
A dialog box is displayed, asking whether you want to verify that the image files exist.
7. Click one of the following options:
 - Click **No** if you are certain that the image files exist.
The **Pgcount** field is updated with new values, or incorrect values are overwritten.
 - Click **Yes** if you want Summation to verify that the image files exist.
Summation verifies the existence of the images and updates the **Pgcount** field. This may take longer than just updating the **Pgcount** field.

Producing eDiscovery from Petrified Documents

Once you have petrified the required documents, you can create your production set and redact the image files as needed. Review Steps 1 – 17 in the *Using Summation to Produce eDiscovery* section of this white paper for instructions on creating your production set, and then return to this section for continued instructions.



To produce eDiscovery from petrified documents:

1. On the **Review Production Set** dialog box, click **Set Production Format**. The Summation layout is formatted to display the column view docked on the top (displaying only those summaries that are associated with eDiscovery), the **Image Viewer** docked on the left, and the **eDocs Viewer** docked on the right. In addition, the **Select Production Mode** dialog box is displayed. The purpose of this dialog box is to give you the opportunity to assign a production format to the documents that you want to produce.

*NOTE: If the case was created in a version previous to Summation Blaze LG/iBlaze Version 2.5, add the **ProdAs** field to the table that your eDiscovery is loaded in.*

2. In the column view, select the document that you want to assign a production format to.
3. On the **Select Production Mode** dialog box, double-click the format that you want to use to produce the selected document. (For this example, select **Redacted (Petrified) Version**.) You can select from the following options:
 - **Electronic Version** – Double-click this option to include the native electronic version of the document (electronic document, e-mail message, or e-mail attachment) in the production set. The **ProdAs** field is set to **2 – eDoc**.
 - **Redacted (Petrified) Version** – Double-click this option to included the petrified and redacted version of the electronic document in the production set. The **ProdAs** field is set to **1 – Image**.
 - **Fully Redacted Document** – Double-click this option to include a fully redacted electronic file (generated by Summation) that is labeled **Fully Redacted Document** in the production set. The **ProdAs** field is set to **0 – Fully Redacted**.
 - **Default Setting** – Double-click this option to include the version of the document specified in the **Production Briefcase Wizard** in the production set. The **ProdAs** field is left blank. This option is overruled if you enter a value in the **ProdAs** field.

*NOTE: If you want to start over, you can clear the **ProdAs** field by clicking **Clear Field**. To clear the **ProdAs** field for multiple summaries, select those summaries and click **Clear Marks**.*

4. Click **Done** when you are finished setting the production formats. A dialog box is displayed, asking you whether you want to save your changes.
5. Click **Yes**. The layout is re-arranged and the **Make Production Set** dialog box is displayed.
6. Continue with Step 19 in the *Using Summation to Produce eDiscovery* section of this white paper for instructions on making redactions and completing production.



Appendix 7: Producing Compound Documents in Summation

The release of Summation Blaze LG/iBlaze Version 2.5 ushers in a new era of eDiscovery functionality. Summation users enjoy unprecedented do-it-yourself functionality to process, load, evaluate, and produce native eDiscovery documents directly to and from Summation.

The Burden of Production

Summation takes substantive discovery requirements to heart when designing tools to facilitate efficient and effective document production. This design philosophy carries through whether you are dealing with any of the following document types:

- Paper
- Paper converted to image format
- Electronic documents in native format
- Electronic documents converted to image format and native electronic format
- Electronic documents converted to image format and extracted full-text, without the native electronic format

Substantively speaking, Summation designs the tools to facilitate the production of those documents, not privileged or otherwise protected from discovery, that are relevant and reasonably calculated to lead to admissible evidence in either of the following ways:

- As maintained in the ordinary course of business
- As asked for by the requesting party
(For more information, see *FED. R. CIV. P 26(B)(1)* and *FED. R. CIV. P 34(b)*).

Electronic Documents in Summation

Electronic documents can be provided in two different formats: document or store.

Document format means the data is maintained in a file for each document. Examples of document file formats include .DOC (Microsoft Word), .XLS (Microsoft Excel), .PDF (Adobe Acrobat), .MSG (Microsoft Outlook), generic .HTML, and ASCII text formatted files, among others. The phrase *each document* can be ambiguous, especially when referring to e-mail messages. From a discovery perspective (among others), when an e-mail message has attachments, it is important to treat the e-mail message and its attachment as a single unit. Therefore, each document has the potential to be a *compound* document, which is discussed in greater detail in the section *Understanding Compound Documents*. Microsoft Outlook recognizes the compound document concept by having a special file type, the .MSG file, which wraps an e-mail message with its attachments into a single file format.

The *store* format is a collection of documents bundled in a single file (for example, e-mail messages in .PST format or single files grouped together in a ZIP file). In addition to containing e-mail messages, e-mail stores may also include attachments, which are documents that are included in an individual e-mail message.



When loaded into Summation, documents in a store format are extracted from the store and treated as individual documents. Documents are designated one of three media types during this process:

- *eDocs*: Evidentiary electronic documents, such as Microsoft Word documents, Excel spreadsheets, or Outlook .MSG files (not supplied within a .PST). When loaded into Summation, a database summary is created for each electronic document.
- *eMail*: Messages located in e-mail stores that are read by e-mail applications, such as Microsoft Outlook or Lotus Notes. When loaded into a Summation case, a database summary is created for each e-mail message.
- *eMail Attachments*: Electronic files (electronic documents or e-mail messages) that are embedded in e-mail messages. When .PST or .NST archive files are loaded into Summation, attachments to e-mail messages are extracted and a database summary is created for each attachment.

Understanding Compound Documents

A document, such as an e-mail message, that has an attachment is called the *parent document*. The attachment is called the *child document*. The parent/child relationship is reflected in the document database summaries. For example, when you look at an original e-mail message in Microsoft Outlook or Lotus Notes, the attachments are an essential part of that e-mail message. Thus, an original e-mail message and its attachments together constitute a complete compound document.

In Summation, although a compound document is separated into several summaries – one for each member that is part of the compound document – a compound document is considered to be one unit. Summation creates a separate summary for each member of the compound document to facilitate coding information about it individually. When viewing a component of a compound document, you can view its related members by using the **Include Family Summaries** function. This function is found on the **Search** menu and under the **Tools** option on the **Summary** menu. It is designed to bring all related members of a compound document into view for easy review. For example, if you have the parent database summary in view, selecting **Include Family Summaries** automatically brings the child attachments into the view.

This functionality helps protect against mistakes. For example, if you perform a search and the results of the that search are found in an attachment to an e-mail message, using **Include Family Summaries** allows you to review the complete compound document and have a fuller understanding of the context of the search hit.

Summation's **Production Tools** use the relational information to produce the entire production set (including attachments in the user-specified format: either native or redacted). This feature is intended to protect against portions of a compound document being inadvertently omitted from a production.

It is extremely important to emphasize that, from the standpoint of discovery production, a compound document is a single, complete document and should be treated as such. The members within the document are simply part of that compound document, not separate and distinct documents per se. As such, Summation is designed with the notion of not violating the structural integrity of the document.



Producing Compound Documents

Summation allows you to designate and electronically apply Bates numbers to native electronic documents for production. Just before Bates number application takes place, the production set is automatically expanded to include the family summaries and bring any family summaries that were omitted into the set. For example, if an e-mail message is included in the production set and its corresponding attachments are not, then all attachments that were originally attached to that e-mail message are automatically added to the documents being produced and assigned a Bates number.

The Summation **Production Tools** are designed to protect the structural integrity of compound documents by automatically including all related items to a document that is designated for production in a production set. Summation does not provide functionality that would permit or facilitate violating the structural integrity of a compound document. However, Summation does allow you to fully or partially redact privileged or protected content as described in the following sections.

Privileged and Protected Documents

Compound documents that are wholly privileged should be marked as such in the database and excluded from the production set and listed in a privilege log.

However, in the event that part of a compound document (such as an attachment) is privileged, then that item should be included as a fully redacted document in the production set. When an e-mail message is produced from the original .PST file, a privileged attachment is replaced with a fully redacted placeholder document to preserve the integrity of the compound document and allow users to exclude privileged information (or items) from it.

If the child document (for example, an attachment) should be produced, but the parent (for example, an e-mail message) is privileged, then the parent should be produced as a petrified and redacted image during the creation of the production set. (For information about petrification and redaction, see the *Petrification and Image Redaction* section.) The child (or attachment) should be included as preferred, native or petrified, in the production set.

Note: Summation allows you to use the petrified or redacted image version of the parent, aggregated into a production **Briefcase** with attachments left in their native formats, or even in an un-redacted image format, if you so choose. In this situation, an e-mail message and its attachments cannot be included in a **PST Briefcase**, but may be included in a **Production Briefcase**.

Petrification and Image Redaction

In the event that you need to redact (partially or completely) a native electronic document, then you can use the Summation **Petrification Toolset** (iBlaze edition only) or ask your service bureau to petrify (convert to TIFF image format) the document, and use the Summation **Image Viewer** markup tools to redact it. The production set will, therefore, include the redacted image version of the native document that is either completely or partially privileged. This also applies to members (for example, an attachment such as a Microsoft Word file) of an .MSG file that is produced as part of a **PST Briefcase**. This functionality ensures that the structural integrity of the compound document is protected, while privileged information is excluded from production.



Appendix 8: Producing E-mail as a .PST File

This appendix covers situations where you may be required to produce e-mail messages in a .PST file. If a .PST was processed in the **eDiscovery Console**, you can proceed to producing e-mail messages in a .PST file.

Note: *Producing e-mail messages in a .PST file differs from creating a Summation production set. Doc IDs are not renumbered with production numbers (Prodno) and Summation does not produce new production IDs (Prodid).*

To produce e-mail messages in a .PST file:

1. Search and retrieve e-mail discovery as outlined in the *Searching and Reviewing eDiscovery* section of this white paper.
2. Double-click **Core Database** in the **Case Explorer**.
The column view is displayed.
3. From the **Search** menu, select **Include Family Summaries**.
OR
From the **Summary** menu, select **Tools** and **Include Family Summaries**.
The **Include Family Summaries** dialog box is displayed.
4. Click **OK** to accept the default settings.
5. Review the parent and child documents for relevance or privilege.
6. Right-click the summary field number and select **Show PST Information**.
The **DocData** window is displayed, showing processing information for the file.
7. If you want to produce only a subset of the e-mail retrieved, mark the summaries associated with the e-mail messages that you want to produce.
8. From the **Summary** menu, select **Production Tools** and **Make an Email (PST) Production**.
A prompt is displayed asking you to confirm that you want to create a .PST file.
9. Click **Yes**.
The **Briefcase coreDB Rows** dialog box is displayed.
10. In the **Enter Name for New Briefcase** box, type a descriptive name for the **Briefcase**, and click **OK**.
The **Briefcase** is created, and a prompt is displayed asking whether you want to load the .PST file into Microsoft Outlook for review or if you want to see the directory where the .PST file is stored.
11. When you are ready to produce the .PST file to opposing counsel or to provide it to a third party (such as an expert witness) for review, copy the .PST file from the location where it is stored to a CD-ROM.



Appendix 9: Using Electronic Evidence in the Deposition Process

Electronic evidence is taking on a dominant role in discovery and regulatory investigation. According to a recent study by the University of California, Berkeley, 93% of all information generated during 1999 was created in digital form on computers, and only 7% originated on paper or other media. Also, more than 10 billion e-mail messages are sent across the Internet and corporate networks each day. By 2006, industry experts expect 60 billion e-mail messages per day to be generated.[†] Given these numbers and projections, the use of e-mail messages and electronic documents will increase considerably. We can, therefore, assume that e-mail messages and electronic documentation will become even more common in the discovery process. They have already permeated discovery practices and the way courts view electronic media.

In the past year, there have been numerous case decisions in both federal and state courts regarding the handling of electronic evidence in litigation. In fact, several states have revised their rules of civil procedure to incorporate electronic evidence as a medium distinct from paper.[‡] Electronic documents are no less subject to disclosure than paper.[§]

Attorneys have already started using electronic evidence in the courtroom. The next logical step is using electronic evidence at depositions, rather than the traditional paper model. Why? One reason is because in addition to the enormous growth of information in electronic format, managing electronic evidence is significantly cheaper in the long run than printed, paper documents. More importantly, unlike paper documents, electronic evidence often contains metadata that can be extremely significant to the case.

The question is not *if* this change will occur, but *when* electronic evidence will become a common form of exhibit used at depositions. On the other hand, this is not to say that electronic forms of documents will wholly replace paper, or that paper does not have its place to memorialize exhibits. The well-versed litigator must be able to objectively determine which media format best suits the task at hand while balancing the many new factors illuminated below in this appendix.

Defining an Electronic Exhibit

First, it is important to understand what constitutes *electronic evidence* versus an *electronic exhibit* used at a deposition.

Several acronyms and terms exist for referring to electronic evidence, such as Electronic Data Discovery (EDD), Electronic Evidence Discovery (EED), and eEvidence, but note that all of these acronyms and terms refer to the same thing. Since electronic evidence is a relatively new topic in litigation, the industry is still finding a common term to describe it. Labels aside, what exactly is electronic evidence?

[†] Kroese, Mark, EDD Showcase: Distinguishing Between Vendors, Law Technology News (2003), available at: http://www.lawtechnews.com/r5/showkiosk.asp?listing_id=399216 (This site requires registration.)

[‡] Several Web sites summarize recent case law and rules regarding electronic evidence, such as <http://www.kenwithers.com>

[§] Simon Property Group, L.P. v. mySimon, Inc., 194 F.R.D. 639 (S.D. Ind. 2000)



The most common forms of electronic evidence are file types that you work with every day in your legal practice: Microsoft Word documents, e-mail messages, and Microsoft Excel spreadsheets. However, electronic evidence also broadly includes digital audio, video, or photographs, as well as program code, database records, and so forth. Thus, writings created, exchanged or archived electronically constitute electronic documents.

Often attorneys think that a document constitutes electronic evidence solely by virtue of being in electronic format. That is not the case. There are differences between exhibit file formats, with some formats having benefits over others.

Comparing Image File Formats to Native File Formats for Deposition Exhibits

This section briefly reviews the characteristics of image file formats and native file formats. Two common image formats are Tagged Image File Format (TIFF) and Portable Document Format (PDF).^{**} If a document is in TIFF or PDF format, it most likely existed as paper or in another file format before it was converted into a TIFF or PDF file using a scanner or PDF-conversion software (typically Adobe Acrobat).

In contrast, the native file format of a document is the format in which it originated. For example, if you request a Microsoft Word document in its native file format, you would receive a file (on CD, floppy disk, or other medium) with a .doc extension. The following are other examples of native file format extensions:

- .PST – A Microsoft file format, .PST files are e-mail files that have been exported from Microsoft Outlook.
- .NSF– An IBM Lotus Notes file format, .NSF files are e-mail files that have been exported from Lotus Notes.
- .XLS – An .XLS file is a Microsoft Excel spreadsheet.

For the purposes of this discussion, the terms *electronic evidence*, *EDD*, and *EED* refer to documents saved in their native file formats, and not as TIFF or PDF files. To *petrify* or *TIFFify* a document means to convert the document from its native format to an image file format for use in litigation. This appendix, however, discusses how deposition exhibits can be in TIFF, PDF, or native file formats in addition to paper, and options and benefits for each.

Native File Format Benefits: The Availability of Metadata

There are numerous reasons why a native file is preferable over a hard copy printout or a TIFF or PDF version of a document. The most significant reason is the valuable metadata associated with it. By far, metadata is the most important and beneficial reason to ask for documents in their native file format in discovery. *Metadata* is defined as follows:

Definitional data that provides information about or documentation of other data managed within an application or environment.^{††}

^{**}Smith, Wayne, *Compare & Contrast: PDF versus TIFF*, Law Technology News (December, 2002) available at: http://www.lawtechnews.com/r5/showkiosk.asp?listing_id=395271&category_id=27902 (This site requires registration.)

^{††} Howe, Denis, *The Free On-line Dictionary of Computing*, copyright 1993, available at: <http://www.foldoc.org> (accessed February, 2004).



In a nutshell, metadata is data that further describes other data. Common examples of metadata include e-mail headers and routing information, formulas in Microsoft Excel spreadsheets, and word processing profiles and editing history.

Metadata in e-mail messages is particularly helpful in establishing timelines – who knew what, when, where, and how. It reveals information that is simply unavailable from the printed hard copy of an e-mail message. For example, metadata can include the date that the e-mail message was sent, received, opened, forwarded, and replied to, and whether it was sent as a blind carbon copy (BCC) to someone. This important information is not detectable in hard-copy form. Yet, if you obtain the same e-mail message in its native file format (such as a .PST file or an .NSF file), you can see that information and more.

Metadata in Microsoft Word documents is especially telling in breach-of-contract cases or any type of case where it is important to ascertain the intent of the parties or whether an agreement has changed over the course of time. The **Statistics** dialog in Microsoft Word allows you to see a wealth of information, including the author of the document, the number of revisions, when it was last saved, when it was printed, and so on. More importantly, any changes made in a Microsoft Word document are easily viewable unless you take certain steps to hide that information (for example, if the Microsoft Word document is converted to a PDF file using Adobe Acrobat Distiller, the metadata from the .doc file is not saved in the PDF). Capturing metadata that reflects drafts, edits, and collaboration is the functional equivalent of capturing every marked-up copy of paper drafts for a paper-based document. This information is another example of metadata that can be extremely valuable in discovery.

TIFF and PDF File Benefits

When an electronic document is converted to TIFF or PDF format, the metadata that was once associated with that document is usually no longer available. This can be good, if you are producing that information, or bad, if you are seeking it.

Consider the metadata that is attached to a Microsoft Word document. Would you want your client to know every revision you've made to a legal document? (This in itself would be a good reason to send PDF instead of Microsoft Word files). On the other hand, wouldn't you want to know the revisions that were made to a contract that has been breached from your opponent?

Scenarios for Using Electronic Exhibits at Depositions

Keep the following considerations in mind when using electronic exhibits at a deposition. First, how will you introduce an exhibit at the deposition? Second, how will that exhibit be distributed to the parties after the deposition?

While this appendix focuses on electronic evidence, a brief discussion of the paper paradigm is in order. Paper still has a place for many reasons, including the following:

- You want to provide opposing counsel with a preview of the exhibit before the witness is exposed.
- You want to provide opposing counsel with a copy of the exhibit so that he or she can read along with the witness during examination.
- You need a copy to capture and fix the mark-ups or margin notes of a witness.

The paper paradigm consists of the following tasks:

- Copying pre-existing paper documents



- Printing native files, such as a Microsoft Word document using the Microsoft Office **Print** function
- Capturing electronic evidence files as TIFF images or PDF files and then printing those out as paper copy

Once that process is completed, the age-old process of dispensing paper-originated documents is carried out: one copy of the converted and/or printed document is given to the reporter to mark and hand to the witness, while the courteous examiner doles out a hard copy to each of the other parties.

The paper paradigm does have substantive shortcomings, the most important of which is loss of information. One of the most important types of lost information resulting from conversion of native electronic files to paper is an accurate depiction of the file related-metadata, such as that contained in an e-mail message or a Microsoft Word file attached to the e-mail message.

The following scenarios present possible situations for using exhibits in TIFF, PDF, or native file formats.

Scenario 1: You want to question the witness about metadata not shown on printed paper or captured in TIFF or PDF files

Envision an instance where you confront a witness with a document that the witness claims not to have seen. Your court reporter, sophisticated in the methods of presenting electronic evidence, brings an extra computer for exhibit display purposes, while you bring a CD-ROM containing the electronic files about which the witness will be questioned. Alternatively, you could bring your own exhibit display computer. The display computer, of course, runs the native applications originally used to create and now display the native electronic evidence files at issue. (Some file types of electronic evidence may require highly specialized software, such as a computer-assisted-design program, to enable the files to be viewed in their native formats on the display computer.)

On the display computer, the witness can now view the document in question in its native file format, which you brought on a CD-ROM. The CD-ROM containing the document can be submitted as an exhibit to the deposition. After the witness denies knowledge of the said document, you use the native application on the display computer (for example, Microsoft Word) to access the file's properties.

If the document was produced by a Microsoft Office product, you can access the file's properties by selecting the **File** menu **Properties** option. A dialog box is displayed with information about the document. Select the **Statistics** tab to see the metadata associated with the document, including the author of the document, the number of revisions, when the document was last saved, when it was printed, and so on.

In this scenario, the metadata indicates that the deponent authored the document. You can now show the deponent (as well as other party representatives in attendance) the display screen that indicates him as the author. You can take a screen shot and print it on a portable printer, or the court reporter can burn a CD of the exhibits for each party. You can also do both: print a screen shot and submit the paper as *Exhibit A-1* and burn a copy of the CD-ROM and mark it as *Exhibit A-2*.

The attorney would bring the exhibits to the deposition in native file format, containing the valuable metadata. If the attorney knows with certainty which documents will be used as exhibits, then all exhibits can be introduced on one CD. However, if there is any question as to whether a particular document can be introduced as an exhibit, you have the option to capture each document separately on an individual CD.



Scenario 2: You've already scanned or converted your case documents into TIFF or PDF files

As litigation support software becomes increasingly popular for managing cases, many attorneys are converting their case documents into TIFF or PDF files as a routine part of their practices. Especially in cases where exhibits are extremely voluminous and/or multiple parties are involved, it is much easier and cheaper to bring along a CD of exhibits to a deposition, rather than lugging banker's boxes full of paper.

In this scenario, the attorney brings a CD with the exhibits in TIFF or PDF format. The court reporter provides an extra computer for exhibit display purposes, running applications that support TIFF or PDF format^{##}. On the display computer, a witness can now view the document in question in its image format, which was made available on the CD.

Scenario 3: You want to establish the parent/child relationships between an e-mail message and a document attachment

An e-mail message and its attachment are generally considered one and the same document. In the litigation support world, an e-mail message with attachments is referred to as a *compound document*. Compound documents exist outside of the e-mail space as well (for example, a brief with appendices). In the paper world, this parent/child relationship is not always evident.

You may want to question a deponent about a particularly relevant, confidential document that he sent to another individual by attaching it to an e-mail message. The deponent admits that he sent an e-mail message to the individual, but denies that he attached the confidential document at issue. In the paper world, it would be difficult to impeach the witness' testimony. However, you could do so easily if you had the e-mail message and its attachment in their native formats at the deposition.

In this scenario, the attorney could demonstrate the parent/child relationship between the e-mail message and its attachment on the display computer.

Scenario 4: After the deposition, you want to receive exhibits in electronic format from the court reporter

It has become common practice for attorneys to receive transcripts in electronic format (such as ASCII, Amicus, or.txt) from the court reporter. It is now possible for court reporters to link the deposition exhibits, and even video, to the electronic transcript so that everything is provided in electronic format. The benefits are enormous, one being that attorneys can immediately view exhibits where they are referenced within the transcript.

The receiving attorney requires specific software to open and review the bundled, linked files. However, this type of software program offers many other transcript-management benefits and features, making it well worth the initial investment.

Attorneys can give the deposition exhibits to the court reporter in either hard copy (which the court reporter will later convert into TIFF or PDF format for the linking process) or on CD-ROM, as outlined in the above scenarios.

^{##} Later versions of Microsoft Windows may contain Kodak© Imaging for Windows Preview or Windows Picture and Fax Viewer, enabling one to view files in TIFF format. Adobe Reader, which is available as a free downloadable program, displays PDF files.



If you are familiar with Summation software (Version 2.5 or later), this bundled file is called the Summation Briefcase Format (**SBF**) file. (For more information about SBF files, see the section *Receiving a Transcript SBF File from the Court Reporter* in this appendix.)

Displaying Electronic Exhibits

The presentation of exhibits in the hypothetical deposition settings in this appendix could take the form of electronic evidence, documents in electronic format, and hard-copy documents, in any combination. Evidence could also be put forward in the form of digital video. The equipment and software required to accommodate the various manifestations of exhibits includes:

- A computer for displaying documents in either electronic format or as electronic evidence and possessing the following features:
 - A monitor for displaying exhibit images and metadata
 - The specific software required to view an electronic document in its native file format (such as Microsoft Word, Outlook, or Excel, Lotus Notes, and so on), thus allowing metadata to be viewed
 - Software for converting electronic evidence from its native format into PDF format for petrification purposes (such as Adobe Acrobat Distiller)
 - Software for viewing image files in PDF and TIFF formats (such as Adobe Acrobat Reader or Windows Picture and Fax Viewer)
 - A CD burner for copying both electronic and electronically-formatted evidence for distribution to opposing counsel
 - A CD-ROM or DVD drive, speakers, and attendant software to present audio and video evidence
- A scanner for converting paper documents image format
- A printer for:
 - Producing paper documents for physical marking by the witness
 - Making physical copies of paper documents (when used in combination with a scanner)

Using Summation for Handling Electronic Exhibits

This appendix has discussed several scenarios above for dealing with electronic exhibits at a deposition. The remainder of this appendix describes the methods for bringing over selected native files or images to the deposition (that is, setting the stage in the litigation support program to make them viewable, manageable, and readily accessible in order to maximize the return on investment in discovery.

Assume that the attorney has Summation iBlaze® (Version 2.5 or later) with native files, as well as TIFFs and PDFs of those documents loaded into the Summation database. Whether you produce or receive exhibits in TIFF, PDF, or native electronic format, Summation can handle it all.

Creating a Browser Briefcase

The Summation **Browser Briefcase** presents data and images in HTML format, and thus is accessible to anyone using an Internet browser, such as Microsoft Internet Explorer.



The **Browser Briefcase** is a great feature for sharing information with a court reporter, expert witnesses, or others who don't have Summation software.

Documents in the **Browser Briefcase** can be TIFF, PDF, and native files. E-mail messages in the **Browser Briefcase** can be .MSG, .PST, or HTML. Additionally, **Browser Briefcases** can include columns of captured fielded information about a document, including certain metadata.^{§§}

In other words, attorneys who create a **Browser Briefcase** can choose the format in which they want to share their documents with other people, depending, for instance, on whether they want to question the witness about metadata.

Receiving a Transcript SBF File from the Court Reporter

The *Summation Briefcase Format* (SBF) file is a file that can contain transcripts (including video synchronization files) and linked, scanned deposition exhibits. Transcript SBF files can be delivered to you by your court reporter by e-mail, diskette, or CD-ROM.

Transcript SBF files allow users of Summation Blaze LG, LG Gold, and iBlaze (Version 2.5 and later) to easily load transcripts and scanned exhibit images using drag-and-drop functionality. The SBF vehicle is the perfect means for receiving transcripts with linked exhibit images in electronic format embodied in the TIFF, JPEG, bitmap, GIF, and PDF file types (as contrasted with electronic documents in their native file formats).

Creating an SBF

The SBF file is created by court reporters using TranSendCR® Plus, a software program licensed at no cost by Summation Legal Technologies. TranSendCR Plus allows the court reporter to complete the following tasks:

- Link exhibits to transcript or video synchronization files
- Create multiple aliases (links) for each exhibit
- Set a password for security purposes
- Create an e-mail message with attorney instructions for loading the SBF file into Summation software or save the file for delivery on diskette or CD-ROM

Benefits of an SBF File

The SBF file can be loaded into the Summation software program with a single command. Benefits of the SBF file include:

- Instantaneous loading of transcripts and video synchronization files, with linked exhibits, in one simple step.
- The entire transcript and exhibits can be viewed and searched immediately upon loading, individually or in tandem, with other transcripts and documents.

^{§§}Summation automatically captures certain metadata when e-mail messages and electronic documents are loaded into the program.



- Each linked exhibit referred to within the transcript can be viewed by clicking on its alias link in the transcript text (for example, *Exhibit 73* or *policy of insurance*).
- Each linked exhibit is assigned a record in the **Core Database**^{***} and can be further coded, viewed, and annotated using Summation's suite of mark-up tools. In addition, you can create an Optical Character Recognition (OCR) of the exhibit on the fly for searching without the need for additional coding.

In summary, the process facilitates setting the stage so the litigation team can realize maximum returns on their investment in depositions and other discovery.

Receiving Electronic Exhibits in Their Native Formats

The following considerations are paramount with respect to the native file. The information that was displayed to the witness should be available:

- For the original records, as well as copies for the other parties, in an immutable form (such as a CD-ROM). As such, the original CD used at the deposition in the display system must be made part of the record and copied for the other parties, to be received along with their paper transcript and electronic transcript file.
- In a format that is conducive for use with litigation support software.

Providing a party with a copy of the CD is straightforward. Providing the native file exhibit in a format that can be most expediently loaded and managed by the litigation support system involves a process. That process can be handled by the court reporting service itself or in conjunction with an eDiscovery service bureau converting the native file format into TIFF or PDF format. Summation refers to this conversion as *petrification*.

Native e-mail files that have been displayed to the witness on the electronic evidence display computer using Microsoft Outlook (after the files had been copied from the CD-ROM disk to the display computer hard drive and, in the case of native .PST, read-only properties of the files removed) require more processing than just petrification. The files must be parsed into their constituent e-mail messages and e-mail attachment files. Then each component of the e-mail – that is, the e-mail message itself and each individual attachment – must be petrified. Once this process is completed, the court reporting agency or service bureau can package the imaged exhibits into the SBF file for inclusion in the litigation support system as set forth in this appendix. The native file on CD would also be available for authentication purposes, if so needed at trial.

Once the native electronic files have been processed as described above, a **Browser Briefcase** can be created and the petrified images can be printed to paper.

If your court reporter cannot process the native files as described above, or you do not have access to a service bureau, you can use the Summation **eDiscovery Console** (LG Gold and iBlaze editions) to process the native document or e-mail files, as set forth in the this white paper. A paralegal could then apply Summation's transcript-linking feature to link the exhibit references in the transcript to the petrified native exhibits.

Creating PDF or TIFF Files (Petrifying Electronic Documents)

Summation iBlaze has the ability to convert documents from their native file format into TIFF or PDF format for instances where you don't want to share the metadata with the opposition or where you want to redact certain content from a document.

^{***} The DocID, DocLink, DocType, and DepoIDs fields of the Core Database are automatically populated with information specifically relating to each exhibit loaded with the transcript SBF method.



Print Copies of Exhibits

You can always print PDF files, TIFF files, and electronic evidence for use at a deposition. However, keep in mind that metadata is often not viewable when you print out a document in its native file format.