

Creating a Positive Outlook for E-Discovery

Tips for managing Microsoft® Exchange and Outlook files throughout the Discovery life cycle.

By D. Douglas Austin

According to studies, the worldwide installed base of e-mail clients will increase from about 1.9 billion “seats” in 2006, to nearly 3.6 billion “seats” in 2010. Microsoft Exchange currently holds a 52% revenue market share of the corporate messaging software market and Outlook commands over 60% of the current installed e-mail client base, with an expected increase to 70% by 2009. E-mail has become the predominant mechanism for written business communications, and Exchange and Outlook are the applications most frequently used to support those communications. Here are several tips regarding Outlook that are important not only for processing, reviewing and producing Outlook content to opposing counsel, but also for the entire discovery process, from planning to production.

Planning Considerations

Retention Policies: Before a case is even filed, the management of Outlook archives can affect your ability to effectively respond to discovery requests. Some organizations have implemented retention policies that incorporate the AutoArchive function of Outlook to automatically archive messages older than a specified time period (e.g., 60 or 90 days). While this approach might reduce the size of the e-mail collection in Exchange databases (.EDB) on the mail server or in offline storage (.OST) mailboxes, custodians often migrate messages to personal storage (.PST) files or individual message (.MSG) files before they are automatically archived. As a result, the policy may only cause Outlook files to become more de-centralized, complicating the collection process. A better solution might be to evaluate and implement an e-mail archiving solution that can support individual custodians’ archive retrieval needs as well as consolidating and streamlining collection for discovery.

Meet and Confer: Also, when a case is filed, several considerations should be addressed when conducting the “meet and confer” with opposing counsel. For example, opposing counsel may be requesting production of Outlook files in their native format, perhaps to ensure that produced files have not been altered. However, because responsive messages are generally stored in a container file (EDB, OST or PST) with all of the other non-responsive messages for one or more custodians, it’s impossible to produce only responsive messages without repackaging those messages into a new container (typically, a PST file). This new container file will have a “create date” later than the relevant time period, so it’s important to establish an understanding with opposing counsel up front regarding production format to avoid spoliation claims. If you’re producing Outlook messages natively, it’s also important to address how redactions of privileged information will be handled. Typically, these are converted to image and redacted since it’s not practical to redact the native Outlook message.

It’s also important to establish an understanding with opposing counsel how various processing issues (mentioned below) will be addressed and handled via exception reports or other mechanisms to keep efforts to address these anomalies to a minimum. Raising these issues at the beginning of the process will save considerable effort and cost downstream.

Collecting Outlook Files

Variety of File Types and Locations: As noted above, there are several different file types associated with Exchange and Outlook. On the server side, EDB files contain mailboxes for multiple custodians and can often be the first place to look for relevant information. Many custodians also have e-mail replicated to an OST file on their local laptop or even to their PDA so that they can access their e-mail remotely when not in the office. Also, custodians often move e-mails into their own personal PST or MSG files which could be stored in a variety of places, from the workstation to various network locations or removable media. To be complete, the collection process must include each of these file types and locations.

Security Mechanisms: The use of security mechanisms, like encryption and password protection, digital signatures and rights management should also be understood up front. The interview and collection process must be comprehensive enough to identify the use of these mechanisms and obtain help from custodians and technical staff to make sure that the files collected can be processed and used for discovery.

Processing Issues

There are several issues that could arise when processing Outlook files that make it difficult to make files available for review and production. These issues include:

Secured and Corrupted Files: As noted above, it is best to coordinate with custodians of encrypted and password protected Outlook files during collection to remove these security mechanisms from the files and facilitate processing. However, this may not always be possible if some custodians of Outlook files are no longer available. Corrupted files can also be a problem and some files cannot be successfully be recovered. Most processing applications cannot successfully extract information from secured Outlook files; therefore, the only way to get to that information is to “crack” the security on those files to retrieve the data. There are several utilities available that can be used to attempt to recover passwords and also to repair corrupted Outlook files; however, successful recovery of these files is not always possible or cost-effective.

Digital Signatures: A digital signature is an electronic, encrypted, authentication stamp on an e-mail or other document, which confirms that it originated from the signer and has not been altered. Issues can arise with opening of attachments from e-mails with digital signatures because the opening of some files can cause the e-mail to be altered, at least temporarily. If any custodians used digital signatures in messages they created, locate samples and confirm that the processing software can support these messages; otherwise, these messages should be included in exception logs provided to opposing counsel of files that cannot be processed.

Links Instead of Attachments: Outlook users often attach various work product files within e-mails to transmit them to intended recipients for review; however, users sometimes insert a hyperlink to the file on the network instead of inserting the file as an attachment in the message. This is done to avoid sending large files through the e-mail system or to require the user to retrieve the file from a secured network share, minimizing the possibility for unauthorized access to the linked file. File links greatly complicate processing since not only is the file not attached to the e-mail, it may no longer even exist.

Time Zone Considerations: Because Outlook displays the messages in the time zone of the user’s workstation, messages sent from east coast users will display three hours earlier on a west coast workstation. This could mean that a message that is sent at 1 AM by an east coast sender could

actually be received a day earlier (10 PM the night before) by a west coast recipient, potentially affecting relevancy date range searches. Select a single time zone most appropriate for the project – e.g., where processing occurs, where the majority of custodians are located, Greenwich Mean Time (GMT), etc. – and document the reasons for using that time zone to satisfy the court that the issue has been addressed.

Deleted Information: When you delete messages within an Outlook folder, they are moved to the Deleted Items folder, where those messages can then be cleared each time you exit Outlook or on demand. Even then, those messages could still exist within deleted item space of the Outlook OST or PST file until the file is compacted. For many users, automatic compaction of these files occurs when running Outlook; however, the possibility exists that some deleted messages may not yet have been compacted when the file is collected.

Rights Management: Information Rights Management (IRM) is a new feature as of Microsoft Office 2003 to prevent sensitive information from being accessed by unauthorized users. In Outlook 2003, users can create and send e-mail messages with restricted permission to help prevent messages from being forwarded, printed, or copied. The same restrictions can also be applied to Office 2003 files attached to Outlook messages. If IRM has been used within your custodians' mailboxes, it may impact your ability to access certain messages within those mailboxes. Coordinate with the custodian and/or technical resources at the custodian's organization to obtain rights to messages or disable IRM for those files.

Again, an agreement with opposing counsel up front to establish parameters for handling problem files and incorporating them into exception logs instead will minimize the effort and cost associated with addressing these issues.

Review of Outlook Files

Native Review: To save discovery costs and reduce production timeframes, it may be desirable to review files in native form and then only convert the relevant messages to image format (or produce them natively) instead of converting the entire custodian's mailbox file. Unlike some e-mail products, such as Lotus Notes, that don't provide an individual message file format, Outlook messages can be extracted to individual MSG files that can be easily reviewed in their native form, with only responsive messages converted and produced to opposing counsel.

Role of Discovery Management Software: Management of the review process is a critical part of effectively reviewing Outlook files and the discovery management software plays a key role. When coordinating multiple reviewers, effective workflow management that provides flexibility in assigning files to reviewers based on a variety of criteria and also provides tracking of review on an individual basis enables each review method to be utilized to the fullest. If there is a need to extract attachments from the Outlook message and produce the individual components of the message separately instead of the entire contents of any message with responsive information, the software should be flexible enough to support this requirement, as well.

Producing Content of Outlook Files

Production Format: The production format should be agreed upon during the meet and confer with opposing counsel, so the production of responsive Outlook messages should simply conform to that agreement. The most common form of production is TIFF or PDF images (the easiest format

to redact and Bates number) along with searchable text and appropriate metadata. When producing Outlook files natively, it's important to determine whether the messages (other than those requiring redaction) will be produced individually as MSG files, or in a repackaged PST container file. In addition to the production of the Outlook messages, an exception log of files that could not be processed should also be provided, along with privilege and production logs that would normally be provided to opposing counsel.

Summary

As you can see, there are several considerations when working with Outlook files that affect the entire discovery life cycle, from pre-litigation planning through production. Knowledge of Outlook's features and capabilities will enable you to avoid potential pitfalls and help ensure a smooth discovery outcome.

D. Douglas Austin is a Technical Consultant at IE Discovery, a provider of comprehensive discovery management solutions. He can be reached at daustin@iediscovery.com.