Forensic Processing of Outlook Email
Recovering Deleted Email Files and Messages
by Kevin Fagalde

If you were to remove the card for a book from the catalog at a library, would you be able to find the book on the shelf? Of course you can! Deleting files from a computer works the same way. Forensic examination of digital media from a laptop, desktop computer, or network server can lead to the recovery of valuable information, including deleted Outlook email messages and attachments, as well as entire deleted personal folder (.pst) files.

Outlook is effectively a database and it stores email messages and attachments as records in an encrypted, compressible format. There are functional limits to the size of an Outlook .pst file, which contains all the personal private folders of the Outlook user. Approaching 2GB file size, the mail must be archived or it will become inaccessible. It is common for corporate users to have an active .pst and several archives if storage quotas are restricted.

Every Outlook user has the ability to delete email messages and their attachments. On a desktop or laptop with Outlook installed as the email client, the ability for Outlook to recover deleted items is only enabled on the Deleted Items folder in a user's private folders. So, if a user deletes an email message inadvertently, it may be easily recovered by the user. In a scenario where an employee sends a company proprietary secret as an email attachment and performs a “hard delete” (by using the SHIFT + DELETE keys) of the message, the user can no longer recover that message. The employee may take it a step farther, by deleting the entire .pst file. However, recovery will still be possible using forensic software tools.

Email messages that are “hard deleted” or those that are deleted from the deleted folder from an Outlook account on a Microsoft Exchange server version 5.5 or later may also be recovered, where the administrator has enabled this feature. Even though hard deleted messages are recoverable from Outlook accounts in Microsoft Exchange server environments, some items or folders may not be recoverable depending on the length of time that deleted items are stored on the server set by the administrator. For public folders, expiration dates take precedence over the length of time set by the administrator.

One factor affecting the ability to recover deleted email is the built-in option for an Outlook user to compact his or her personal folders file. Though a fragment of the pre-compacted .pst file may exist in unallocated space on the hard drive, the fragment will not have any viewable text, since the default setting is to have the data stored in a compressible encrypted format.

The prospect of data recovery on a server really begins with the policies and settings put into place upon installation. Network administrators must be aware of the needs of the organization to recover critical data so hardware and software installations are properly configured up front to

maximize the ability to recover critical data. There are many Internet resources available for managers, so they may develop corporate email use policies and properly setup and administer Outlook email and Microsoft Exchange.