Recovery of Deleted Outlook Express Email Messages from an EnCase e01 Image

The research and development that went into recovering Outlook Express email was almost as considerable as it was for AOL email.

To recover Outlook Express messages from a disk image, the software has to ignore the normal structures of the DBX file. These structures point to the data blocks. This means a complicated search and validation engine had to be developed to ensure that this was done correctly and efficiently.

The design goal for this module was to recover live and deleted email messages from a disk image where the file index was missing or corrupt. This would allow individual email messages to be recovered. It is impossible for a simple traditional carver to be able to recover this type of file correctly as the data is split into blocks which contain email data and other binary information. It is also highly likely that the data will not be in contiguous blocks.

This video demonstrates how to recover live and deleted Outlook Express (version 5 and 6) email messages directly from an EnCase image.