Recovery of Microsoft Outlook Express Email Messages

Overview

This Professional Recovery Module has the ability to recover live and deleted email messages (including attachments) whether directly from a Forensic image (such as an Encase® e01 compressed image) or a physical disk / volume. The output from the software allows the forensic investigator to identify the exact location the data was recovered from. The carving engine for this Module (and the AOL Professional Recovery Module) is the result of numerous years research and development. It was originally released in the Digital Detective product EMLXtract. This product has been used by law enforcement agencies all round the world to recover deleted Outlook Express data since 2004.

Recovery Methodology

Recovering deleted Outlook Express email messages (a similar methodology is required for Microsoft Windows Mail) is not a simple process. It cannot be done with simple header/footer carving. The recovery methodology is outlined in the following document, which was first presented to digital forensic practitioners from law enforcement at the ACPO (Association of Chief Police Officers) Conference at Wyboston in 2004.

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