Recovery of AOL PFC Email Messages from a Segmented Disk Image

The research and development that went into recovering AOL email messages from a forensic image took a considerable amount of time. AOL email messages contain many different elements such as compressed and non-contiguous data blocks. Embedded attachments can be split and have to be stitched back together. When this module was originally designed, the goal was not to recover live and deleted email messages from a Personal Filing Cabinet, but to be able to recover emails from a disk image. This functionality was originally released to Police Forces all around the world as a tool called EMLXtract.Through research and development, the recovery engine has been enhanced further and is now part of Blade. This video shows the extraction and examination of AOL email messages from a segmented disk image.