Recovery of AOL Personal Filing Cabinet Email Messages

The AOL Professio nal Recovery Module (included with Blade® Professional) has the ability to recover live and deleted email messages (including attachments) directly from:

- Forensic images (such as an Encase® e01 compressed images, dd, segmented and AFF)
- Physical disks and volumes
- AOL PFC (Personal Filing Cabinet) file

The output from the software allows the forensic investigator to identify the exact location the data was recovered from.

History

The carving engine for this Professional Module was originally released in the Digital Detective product EMLXtract. When this software was released to law enforcement practitioners in 2004, it was the first forensic tool to recover AOL email messages from an image or physical/logical device. When compared against other tools, this software recovered more email messages than any other. It works particularly well against corrupted data when many other tools fail to recover anything at all. This professional module uses our Intelli-Carve® technology to piece different parts of the message back together again and validates the data in the process. The software also has the ability of recovering inline image attachments. It is particularly good at recovering isolated email messages from unallocated clusters and other areas where deleted messages may reside.

AOL Email Messages

AOL email messages contain many different elements such as compressed and non-contiguous data blocks; as the data is compressed, traditional keyword searching will fail.

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. The following video shows the extraction and examination of AOL email messages from a segmented disk image:

Output from Blade

As the original AOL email data is in a bespoke format designed to be viewed inside the AOL software, Blade recovers each message and creates a representation of the original email message is HTML format. The file can then be viewed (including any embedded image) with a standard browser.

⚠ Please note: Blade does not recreate the email in AOL PFC format, so you cannot view the recovered messages within the AOL client. Figure 1 below shows the output from a single AOL message.
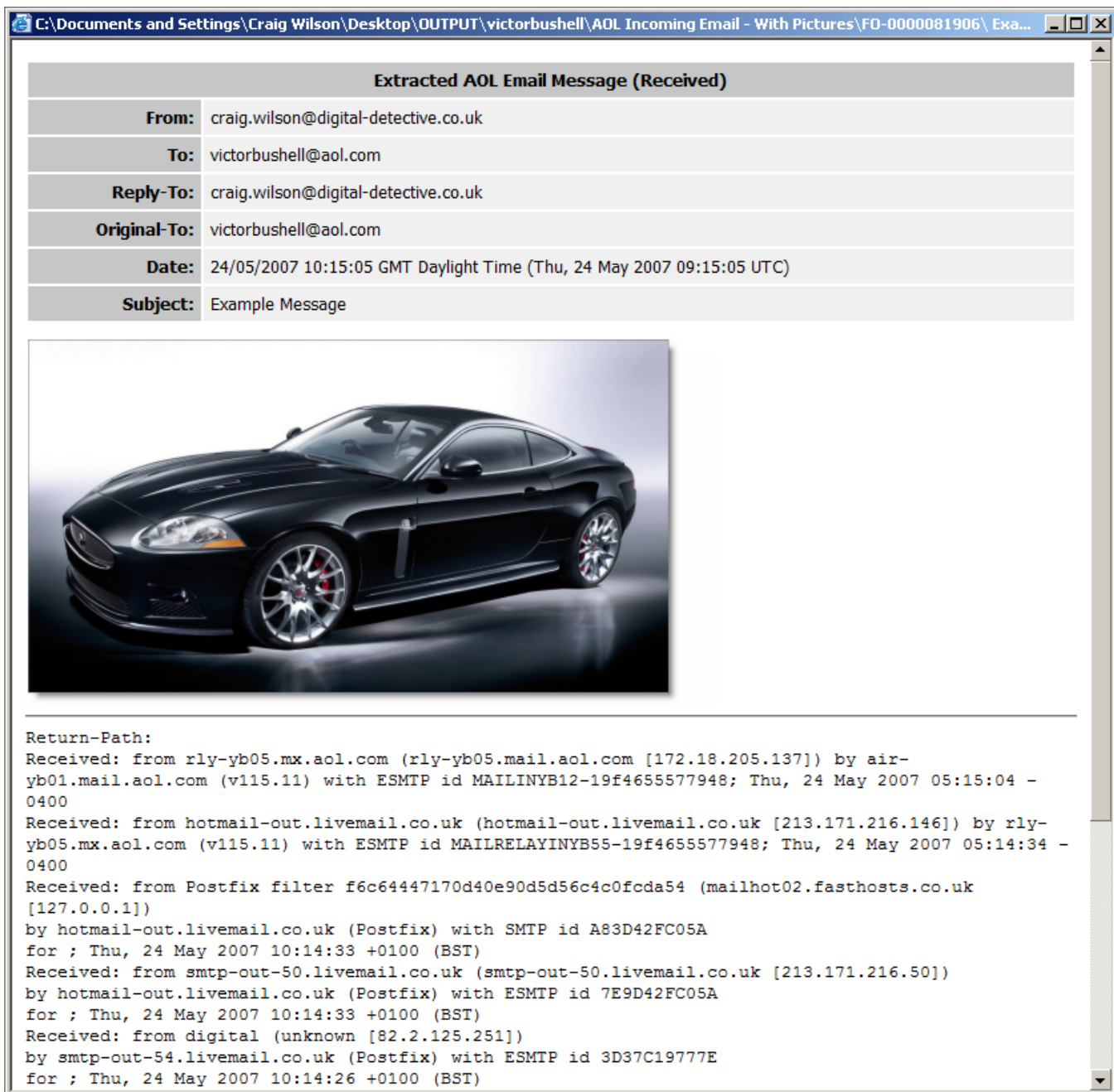
Figure 1

To recover data directly from a hard disk, please follow the instructions in the Blade Quick Start Guide.