

EnCase e01 Segments larger than 2 GiB

Problem

In EnCase 6.7, a change was made to the structure of the e01 evidence file so that segment files greater than 2 GiB could be employed.

Prior to 6.7, the maximum permissible segment size was 2 GiB. This was due to an addressing limitation in the segment files. Each segment file maintains a number of tables which contain an array of 32 bit integers. Each 32 bit integer points to a location within the segment file where the data is located. The most significant bit of each integer is used to flag whether the data block is Zlib compressed or not, which limits the maximum addressable data offset to 2^{31} , hence the 2 GiB segment size limit. To allow the data beyond this limit to be addressable, a 64 bit base offset is added to each table section thereby increasing the maximum addressable offset. This has the added benefit of increasing the potential segment file size to 64 bits whilst not actually making any significant changes to the structure of the tables.

Solution

Blade v1.7+ has now been updated to support single segment e01 image files which are greater than 2 GiB.