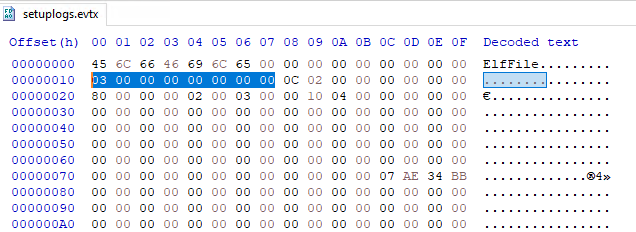
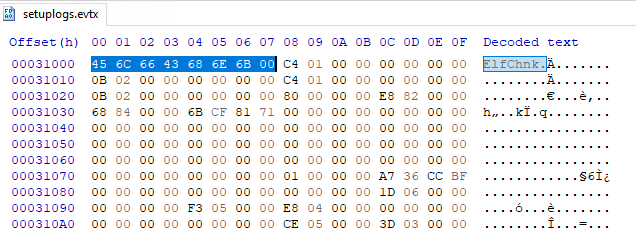
**Log Scrubbing Lab - Brian Guerrero**

LastChunkNumber (Active Chunk) = 03

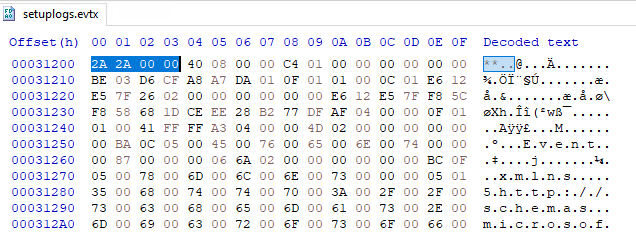


Active chunk offset = 4096 + (3 \* 65536) = 200704 = 31000h

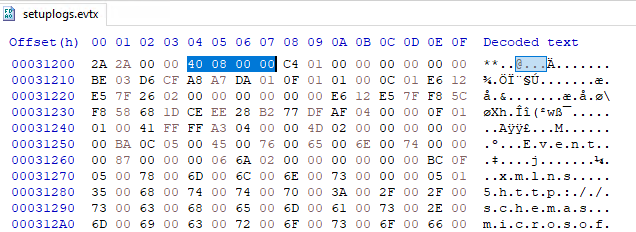
31000h: EVTX\_CHUNK\_HEADER



31000h + 200h (header size) = 31200h, EVTX\_EVENT\_RECORD (first record)

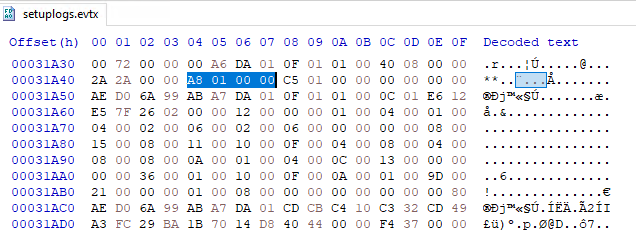


First Record Size = 0840h



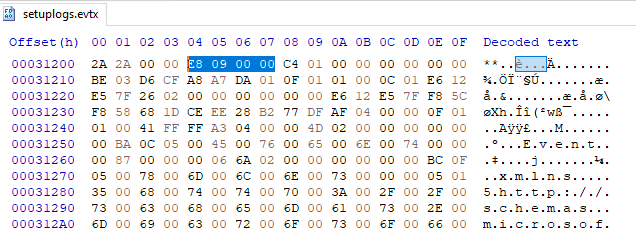
31200h + 840h = 31A40h (second record)

Second Record Size = 01A8h

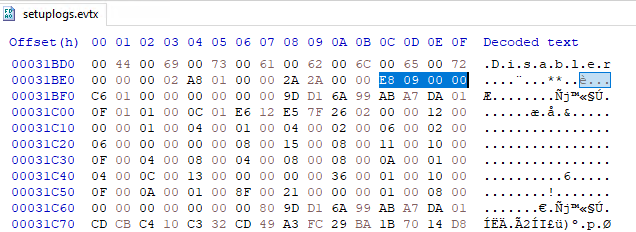


840h (First Record Size) + 1A8h (Second Record Size) = 9E8h

Edit First Record Size at Start of Record



Edit Second Record Size at End of Record (31200h + 9E8h = 31BE8h)



Second Record is now hidden!