

Lab 2

Strategy

I originally studied the “ZSTATS.OVL” file because I thought the title meant it contained the stats of the game. After struggling, I gave up and decided to check other files. When I checked “SAVED.GAM,” it looked like it would have stats on my character since my name and the other companion’s names were shown in text on the right side (using Hex Fiend). As I scanned row 0, the hex values matched up with my Str, Int, Dex...etc. I then converted the decimal values (99, 999, & 9999) to hex and replaced it correspondingly. To change the hex values that take up more than 2 digits, I had to figure out the arrangement so that it would give me the right value. For example, to change the HP to 999, I converted it to hex which is 73E but in Hex Fiend, I had to format it to E703. I did the same thing for HM, EXP, and Gold. I continued to use the same strategy for items. I converted the item values (in decimal) in the game to hex and looked for a sequence in the binary file. For items that did not exist in the game yet (black badge, magic carpets...etc), I had to put 1’s on the 0’s to see which items pop-up in the game until I saw what I needed. I then changed their values to whatever the prompt requested.

Offsets (for main character)

- Str: byte 14, changed 4147**14**15 to 4147**63**15
- Dex: byte 15, changed 414763**15** to 414763**63**
- Int: byte 16, changed **14**143C00 to **63**143C00
- Magic: byte 17, changed 63**14**3C00 to 63**63**3C00
- HP: byte 18 & 19, changed 6363**3C00** to 6363**E703**
- HM: byte 20 & 21, changed **3C00**9600 to **E703**9600
- Exp: byte 22 & 23, changed E703**9600** to E703**0F27**
- Gold: byte 516 & 517, changed **9600**0200 to **0F27**0200

For the companions, I just added 32 bytes (since each line is 32 bytes long) to each preceding character in the list to find the appropriate byte for an attribute.

- keys: byte 518, changed 0F27**02**00 to 0F27**64**00
- gems: byte 519, changed 0F2764**00** to 0F2764**64**
- skull keys: byte 523, changed 040000**00** to 040000**64**
- black badge: byte 536, changed **00000000** to **01000000**
- magic carpet: byte 522, changed 0400**00**64 to 0400**02**64
- magic axe: byte 576, changed **00000000** to **0A000000**

Screenshots



