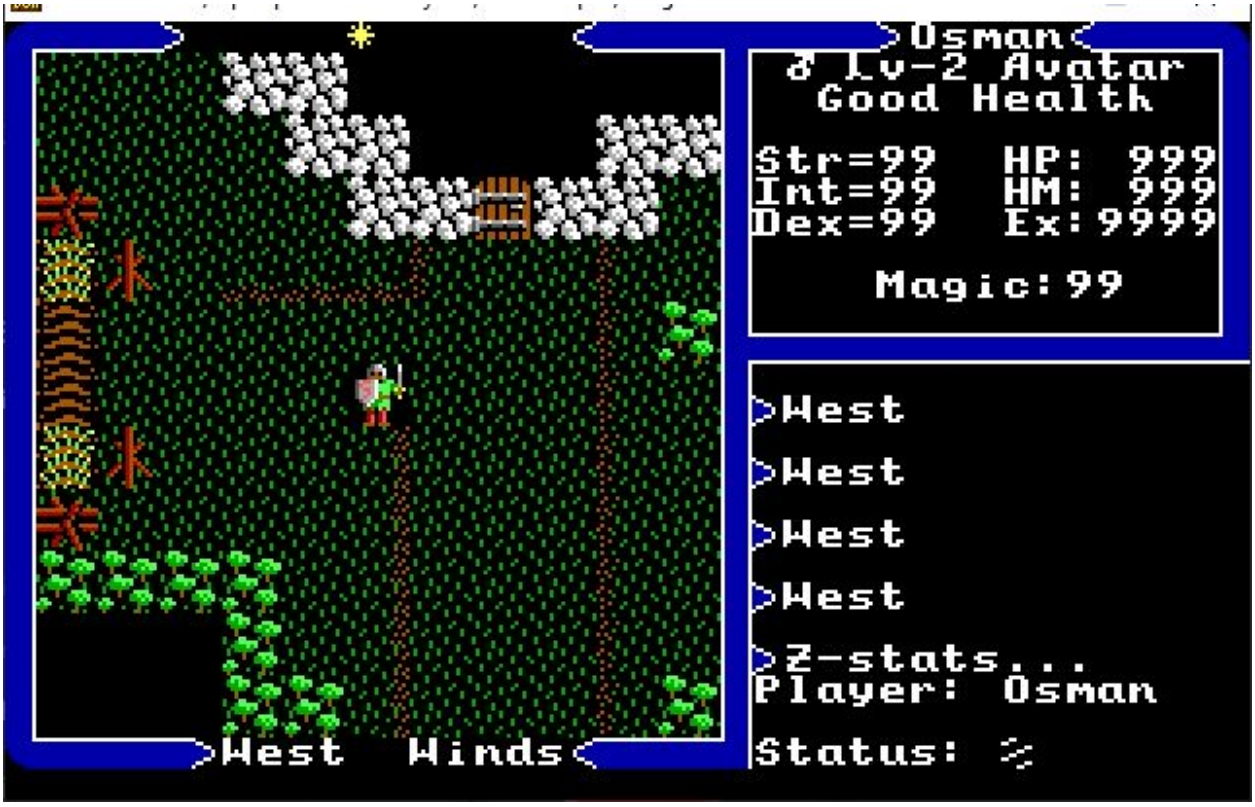
Osman Khan

Lab 2 Report

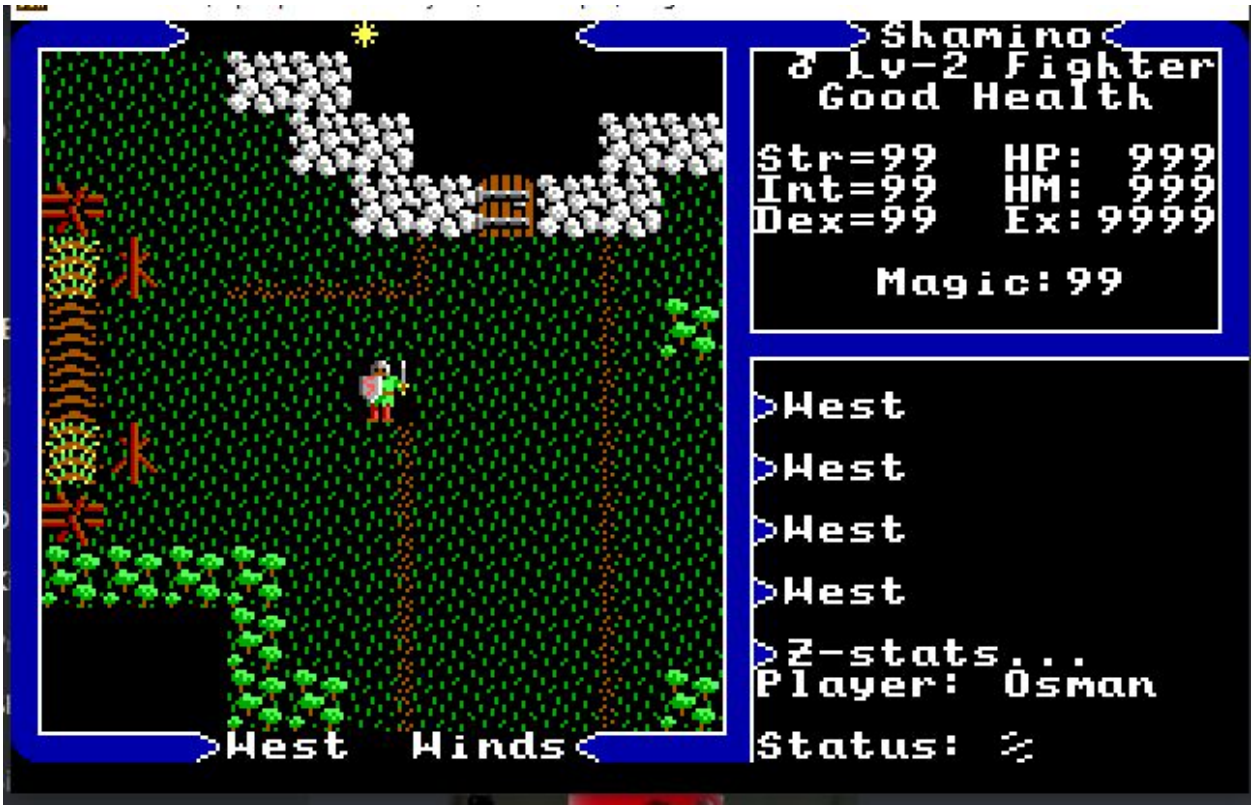
I used the HxD hex editor to edit the SAVED.GAM file located in the Ultima folder in order to edit the character stats and item count in game. The way I determined which file to alter was finding the save file in the Ultima folder and seeing it had the characters' names as the decoded text. Once I converted the file to display the offsets in sets of 32 bytes and changed the view of the file to DOS/IBM-ASCII (OEM) it became more apparent what offsets to edit. I noticed the first two offsets for the main character were unused, or used for some other purpose, and the same was applied to all characters. There was a symbol for the character's gender and the following offset matched the character's strength, intelligence, dexterity, and other character related stats. Some values were only a single byte such as strength, but values such as health points were a word and took up 2 bytes of space which allowed it to be a value greater than 255. This pattern was the same for every character and I replicated it for the entire party. Once I had completed the characters stats for everyone I moved on to the next line of offsets. This started on the offset 200 and I kept the pattern of the first two offsets being unused or used for something else. From there I saw what values could possibly represent the gold my party had. Once I found where it was located it was also a word that included two bytes. From there I located where the other item representations could be through trial and error. The Black Badge was more tricky because it wasn't a numbered item, but something the party has or doesn't. Once I learned where it was located in the offset I set it to the max value for a single byte.

Screenshots

Player Character stats:

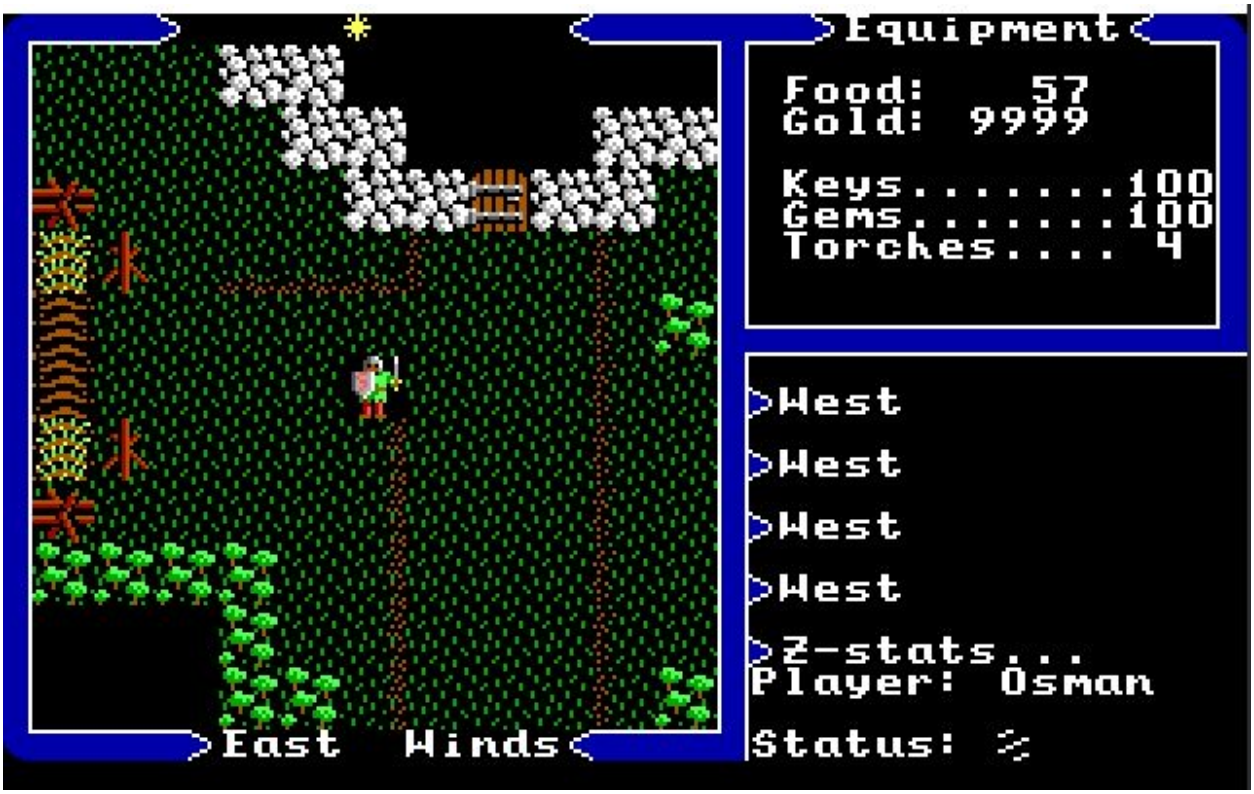


Shamino stats:

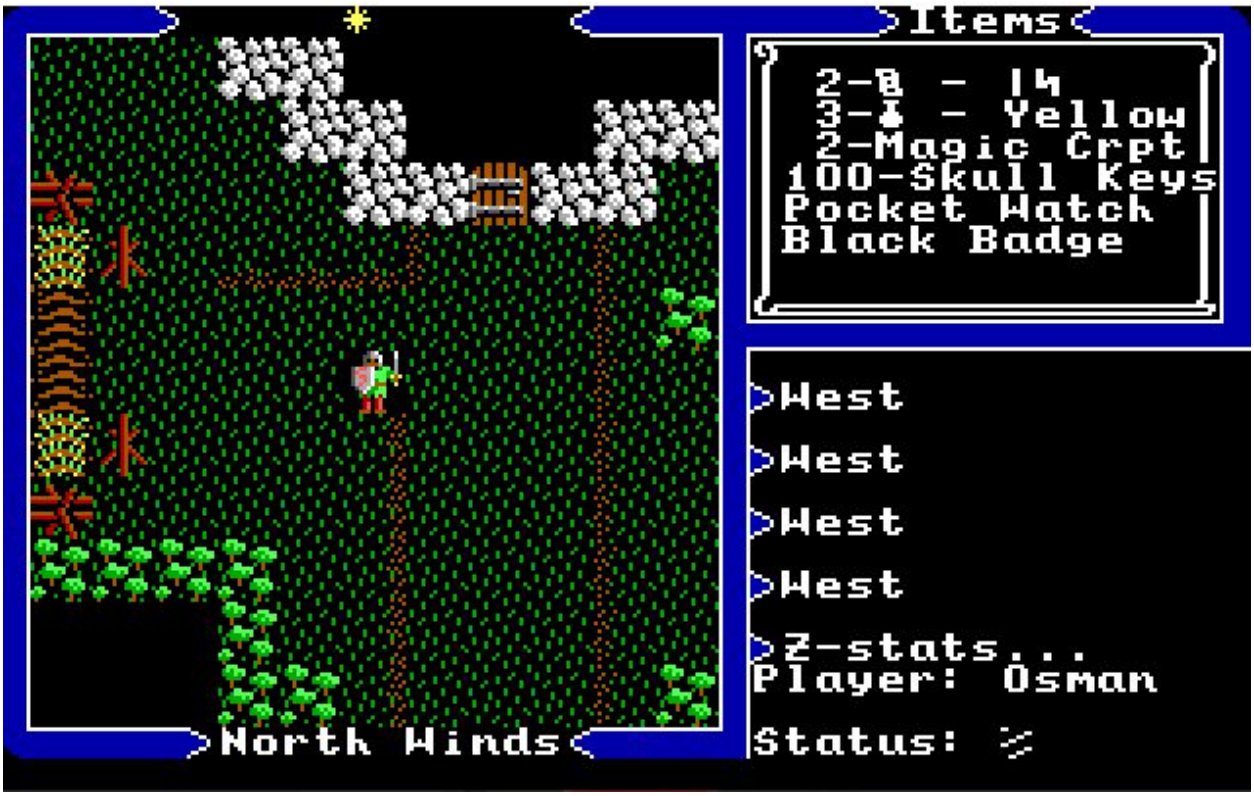


Party Stats:

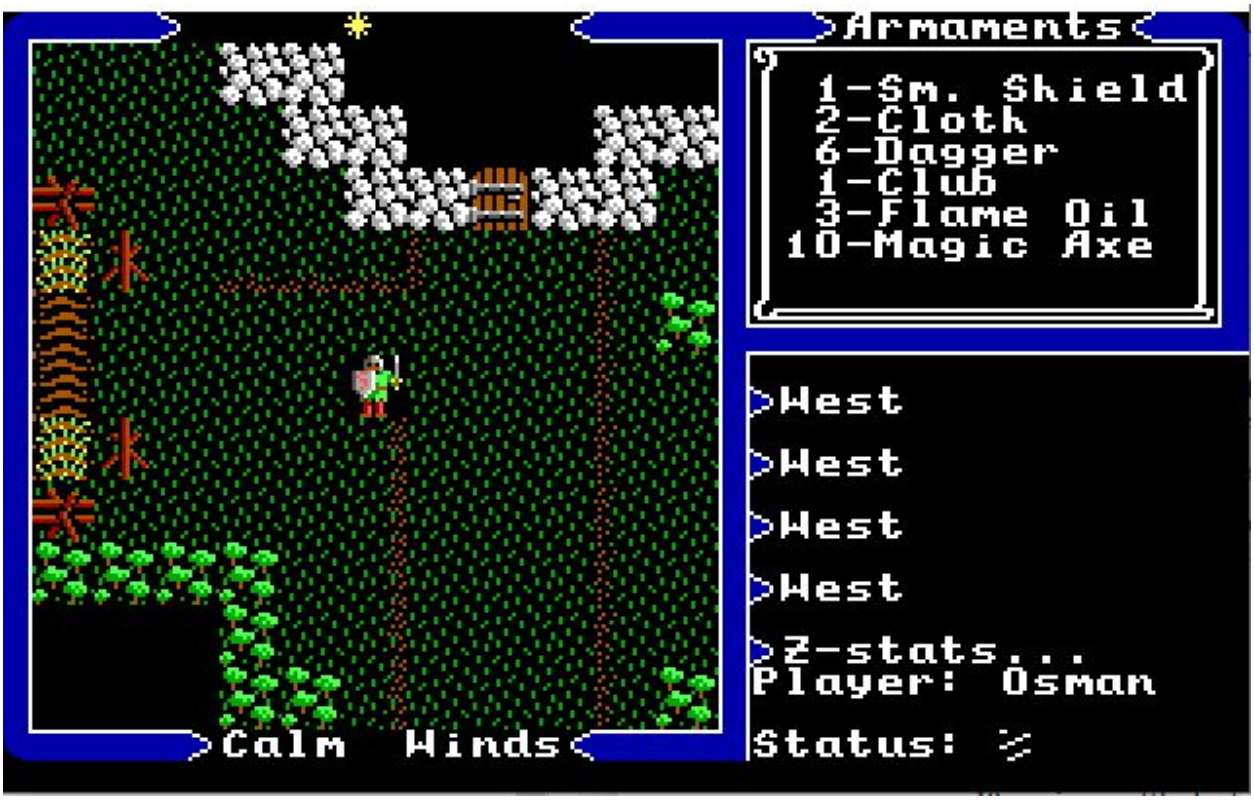
Keys and Gems:



Skully Keys Magic Carpet and Black Badge:



Magic Axes:



Hex Offsets

Osman starts @ 0x00000002
- **str = 20 -> 99 @ 63 hex offset :0x0000000E**
- **int = 21 -> 99 @ 63 hex offset :0x00000010**
- **dex = 16 -> 99 @ 63 hex offset :0x0000001F**
- **hp = 60 -> 999 @ E7 03 hex offset :0x00000012 & 0x00000013**
- **hm = 60 -> 999 @ E7 03 hex offset :0x00000014 & 0x00000015**
- **ex = 150 -> 9999 @ 0F & 27 hex offset :0x00000016 & 0x00000017**
- **magic = 21 -> 99 @ 63 hex offset :0x00000011**

Shamino starts @ 0x00000022
- **str = 20 -> 99 @ 63 hex offset :0x0000002E**
- **int = 16 -> 99 @ 63 hex offset :0x00000030**
- **dex = 22 -> 99 @ 63 hex offset :0x0000002F**
- **hp = 5 -> 999 @ E7 03 hex offset :0x00000032 & 0x00000033**
- **hm = 60 -> 999 @ E7 03 hex offset :0x00000034 & 0x00000035**
- **ex = 167 -> 9999 @ 0F & 27 hex offset : 0x00000036 & 0x00000037**
- **magic = 0 -> 99 @ 63 hex offset :0x00000031**

Iolo starts @ 0x00000042

str = 19 -> 99 @ 63 hex offset :0x0000004E
int = 17 -> 99 @ 63 hex offset :0x00000050
dex = 21 -> 99 @ 63 hex offset :0x0000004F
hp = 90 -> 999 @ E7 03 hex offset :0x00000052 & 0x00000053
hm = 90 -> 999 @ E7 03 hex offset :0x00000054 & 0x00000055
ex = 249 -> 9999 @ 0F & 27 hex offset : 0x00000056 & 0x00000057
magic = 8 -> 99 @ 63 hex offset :0x00000051

Mariah starts @ 0x00000062

str = 12 -> 99 @ 63 hex offset :0x0000006E
int = 22 -> 99 @ 63 hex offset :0x00000070
dex = 20 -> 99 @ 63 hex offset :0x0000006F
hp = 90 -> 999 @ E7 03 hex offset :0x00000072 & 0x00000073
hm = 90 -> 999 @ E7 03 hex offset :0x00000074 & 0x00000075
ex = 249 -> 9999 @ 0F & 27 hex offset : 0x00000076 & 0x00000077
magic = 22 -> 99 @ 63 hex offset :0x00000071

Geoffery starts @ 0x00000082

str = 12 -> 99 @ 63 hex offset :0x0000008E
int = 22 -> 99 @ 63 hex offset :0x00000090
dex = 20 -> 99 @ 63 hex offset :0x0000008F
hp = 90 -> 999 @ E7 03 hex offset :0x00000092 & 0x00000093
hm = 90 -> 999 @ E7 03 hex offset :0x00000094 & 0x00000095
ex = 249 -> 9999 @ 0F & 27 hex offset : 0x00000096 & 0x00000097
magic = 22 -> 99 @ 63 hex offset :0x00000091

Jaana starts @ 0x000000A2

str = 12 -> 99 @ 63 hex offset :0x000000AE
int = 22 -> 99 @ 63 hex offset :0x000000B0
dex = 20 -> 99 @ 63 hex offset :0x000000AF
hp = 90 -> 999 @ E7 03 hex offset :0x000000B2 & 0x000000B3
hm = 90 -> 999 @ E7 03 hex offset :0x000000B4 & 0x000000B5
ex = 249 -> 9999 @ 0F & 27 hex offset : 0x000000B6 & 0x000000B7
magic = 22 -> 99 @ 63 hex offset :0x000000B1

Julia starts @ 0x000000C2

str = 12 -> 99 @ 63 hex offset :0x000000CE
int = 22 -> 99 @ 63 hex offset :0x000000D0
dex = 20 -> 99 @ 63 hex offset :0x000000CF
hp = 90 -> 999 @ E7 03 hex offset :0x000000D2 & 0x000000D3
hm = 90 -> 999 @ E7 03 hex offset :0x000000D4 & 0x000000D5
ex = 249 -> 9999 @ 0F & 27 hex offset : 0x000000D6 & 0x000000D7
magic = 22 -> 99 @ 63 hex offset :0x000000D1

Dupre starts @ 0x000000E2
str = 12 -> 99 @ 63 hex offset :0x000000EE
int = 22 -> 99 @ 63 hex offset :0x000000F0
dex = 20 -> 99 @ 63 hex offset :0x000000EF
hp = 90 -> 999 @ E7 03 hex offset :0x000000F2 & 0x000000F3
hm = 90 -> 999 @ E7 03 hex offset :0x000000F4 & 0x000000F5
ex = 249 -> 9999 @ 0F & 27 hex offset : 0x000000F6 & 0x000000F7
magic = 22 -> 99 @ 63 hex offset :0x000000F1

Katrina starts @ 0x00000102
str = 12 -> 99 @ 63 hex offset :0x0000010E
int = 22 -> 99 @ 63 hex offset :0x00000110
dex = 20 -> 99 @ 63 hex offset :0x0000010F
hp = 90 -> 999 @ E7 03 hex offset :0x00000112 & 0x00000113
hm = 90 -> 999 @ E7 03 hex offset :0x00000114 & 0x00000115
ex = 249 -> 9999 @ 0F & 27 hex offset : 0x00000116 & 0x00000117
magic = 22 -> 99 @ 63 hex offset :0x00000111

Sentri starts @ 0x00000122
str = 12 -> 99 @ 63 hex offset :0x0000012E
int = 22 -> 99 @ 63 hex offset :0x00000130
dex = 20 -> 99 @ 63 hex offset :0x0000012F
hp = 90 -> 999 @ E7 03 hex offset :0x00000132 & 0x00000133
hm = 90 -> 999 @ E7 03 hex offset :0x00000134 & 0x00000135
ex = 249 -> 9999 @ 0F & 27 hex offset : 0x00000136 & 0x00000137
magic = 22 -> 99 @ 63 hex offset :0x00000131

Gwenno starts @ 0x00000142
str = 12 -> 99 @ 63 hex offset :0x0000014E
int = 22 -> 99 @ 63 hex offset :0x00000150
dex = 20 ->99 @ 63 hex offset :0x0000014F
hp = 90 -> 999 @ E7 03 hex offset :0x00000152 & 0x00000153
hm = 90 -> 999 @ E7 03 hex offset :0x00000154 & 0x00000155
ex = 249 -> 9999 @ 0F & 27 hex offset : 0x00000156 & 0x00000157
magic = 22 ->99 @ 63 hex offset :0x00000151

Johne starts @ 0x00000162
str = 12 -> 99 @ 63 hex offset :0x0000016E
int = 22 -> 99 @ 63 hex offset :0x00000170
dex = 20 -> 99 @ 63 hex offset :0x0000016F
hp = 90 -> 999 @ E7 03 hex offset :0x00000172 & 0x00000173
hm = 90 -> 999 @ E7 03 hex offset :0x00000174 & 0x00000175
ex = 249 ->9999 @ 0F & 27 hex offset : 0x00000176 & 0x00000177

magic = 22 ->99 @ 63 hex offset :0x00000171

Gorn starts @ 0x00000182
str = 12 -> 99 @ 63 hex offset :0x0000018E
int = 22 ->99 @ 63 hex offset :0x00000190
dex = 20 -> 99 @ 63 hex offset :0x0000018F
hp = 90 ->999 @ E7 03 hex offset :0x00000192 & 0x00000193
hm = 90 -> 999 @ E7 03 hex offset :0x00000194 & 0x00000195
ex = 249 ->9999 @ 0F & 27 hex offset : 0x00000196 & 0x00000197
magic = 22 -> 99 @ 63 hex offset :0x00000191

Maxwell starts @ 0x000001A2
str = 12 -> 99 @ 63 hex offset :0x000001AE
int = 22 ->99 @ 63 hex offset :0x000001B0
dex = 20 -> 99 @ 63 hex offset :0x000001AF
hp = 90 -> 999 @ E7 03 hex offset :0x000001B2 & 0x000001B3
hm = 90 -> 999 @ E7 03 hex offset :0x000001B4 & 0x000001B5
ex = 249 -> 9999 @ 0F & 27 hex offset : 0x000001B6 & 0x000001B7
magic = 22 -> 99 @ 63 hex offset :0x000001B1

Toshi starts @ 0x000001C2
str = 12 ->99 @ 63 hex offset :0x000001CE
int = 22 ->99 @ 63 hex offset :0x000001D0
dex = 20 -> 99 @ 63 hex offset :0x000001CF
hp = 90 -> 999 @ E7 03 hex offset :0x000001D2 & 0x000001D3
hm = 90 -> 999 @ E7 03 hex offset :0x000001D4 & 0x000001D5
ex = 249 ->9999 @ 0F & 27 hex offset : 0x000001D6 & 0x000001D7
magic = 22 ->99 @ 63 hex offset :0x000001D1

Sadju starts @ 0x000001E2
str = 12 ->99 @ 63 hex offset :0x000001EE
int = 22 ->99 @ 63 hex offset :0x000001F0
dex = 20 ->99 @ 63 hex offset :0x000001EF
hp = 90 -> 999 @ E7 03 hex offset :0x000001F2 & 0x000001F3
hm = 90 -> 999 @ E7 03 hex offset :0x000001F4 & 0x000001F5
ex = 249 -> 9999 @ 0F & 27 hex offset : 0x000001F6 & 0x000001F7
magic = 22 -> 99 @ 63 hex offset :0x000001F1

Gold(word) = 150 -> 9999 @ 0F & 27 hex offset :0x00000204 & 0x00000205
original offset = 96 & 00

Keys = 02 -> 100 @ 64 hex offset :0x00000206
original offset = 02

Skull Keys = 00 -> 100 @ 64 hex offset :0x0000020B
original offset = 00

Gems = 00 -> 100 @ 64 hex offset :0x00000207
original offset = 00

Black Badge = 00 -> 01 @ FF hex offset :0x00000218
original offset = 00

Magic Carpet = 00 -> 02 @ 02 hex offset :0x0000020A
original offset = 00

Magic Axe = 00 -> 10 @ 0A hex offset :0x00000240
original offset = 00