Steven Dao
Prof. Anthony Giacalone

Lab 2 Report

Write-up:

In determining which file to alter, I noticed that the “SAVED.GAM” file was the best candidate for manipulating the in-game values, as it was the only file I could find that would be consistently updated. Once I started checking through the bytes within the file using the HxD hex editor, I thought it would be wise to look for the values representing “OKAMI” in hex since that was the name of my character (and luckily enough, it was shown in the text description within the editor as well). I then started to look for the in-game values of the stats, such as STR=22 or INT=16 in their hexadecimal counterparts, which allowed me to find the offsets most likely responsible for the character stats.Some stat manipulations took multiple tries in order to determine that they occupied multiple offsets (ie. HP, EXP). I then repeated this process for all 16 characters, since they were identically placed in consecutive rows, and was able to essentially copy/paste the altered bytes once I distinguished the pattern.

Finding the offsets for the rest of the items/equipment took a considerably greater amount of trial and error. I altered one byte at a time and proceeded to restart the game after each minor modification to the “SAVED.GAM’ file. After altering the incorrect offsets, sometimes the game would lag on startup, and at one point, my character was even spawning into a lake coordinate, causing the character to drown on startup. Once I found the correct offsets in which the item/equipment I was looking for had successfully appeared in my inventory, I had to change the hex value at that offset to match what was required for the hacked game. Overall, I had a lot of fun dissecting the data of the game and learning about its organization.

Offsets modified:

Data	Offset 1	Offset 2	Offset 3	Offset 4	Offset 5	Offset 6	Offset 7	Offset 8
Char 1	0xE (STR)	0xF (INT)	0x10 (DEX)	0x11 (MAG)	0x12 - 0x13 (HP)	0x14 - 0x15 (HM)	0x16 - 0x17 (EXP)	0x18 (EXP)
Char 2	0x2E (STR)	0x2F (INT)	0x30 (DEX)	0x31 (MAG)	0x32 - 0x33 (HP)	0x34 - 0x35 (HM)	0x36 - 0x37 (EXP)	0x38 (EXP)
Char 3	0x4E (STR)	0x4F (INT)	0x50 (DEX)	0x51 (MAG)	0x52 - 0x53 (HP)	0x54 - 0x55 (HM)	0x56 - 0x57 (EXP)	0x58 (EXP)
Char 4	0x6E (STR)	0x6F (INT)	0x70 (DEX)	0x71 (MAG)	0x72 - 0x73 (HP)	0x74 - 0x75 (HM)	0x76 - 0x77 (EXP)	0x78 (EXP)
Char 5	0x8E (STR)	0x8F (INT)	0x90 (DEX)	0x91 (MAG)	0x92 - 0x93 (HP)	0x94 - 0x95 (HM)	0x96 - 0x97 (EXP)	0x98 (EXP)
Char 6	0xAE (STR)	0xAF (INT)	0xB0 (DEX)	0xB1 (MAG)	0xB2 - 0xB3 (HP)	0xB4 - 0xB5 (HM)	0xB6 - 0xB7 (EXP)	0xB8 (EXP)
Char 7	0xCE (STR)	0xCF (INT)	0xD0 (DEX)	0xD1 (MAG)	0xD2 - 0xD3 (HP)	0xD4 - 0xD5 (HM)	0xD6 - 0xD7 (EXP)	0xD8 (EXP)
Char 8	0xEE (STR)	0xEF (INT)	0xF0 (DEX)	0xF1 (MAG)	0xF2 - 0xF3 (HP)	0xF4 - 0xF5 (HM)	0xF6 - 0xF7 (EXP)	0xF8 (EXP)
Char 9	0x10E (STR)	0x10F (INT)	0x110 (DEX)	0x111 (MAG)	0x112 - 0x113 (HP)	0x114 - 0x115 (HM)	0x116 - 0x117 (EXP)	0x118 (EXP)
Char 10	0x12E (STR)	0x12F (INT)	0x130 (DEX)	0x131 (MAG)	0x132 - 0x133 (HP)	0x134 - 0x135 (HM)	0x136 - 0x137 (EXP)	0x138 (EXP)
Char 11	0x14E (STR)	0x14F (INT)	0x150 (DEX)	0x151 (MAG)	0x152 - 0x153 (HP)	0x154 - 0x155 (HM)	0x156 - 0x157 (EXP)	0x158 (EXP)
Char 12	0x16E (STR)	0x16F (INT)	0x170 (DEX)	0x171 (MAG)	0x172 - 0x173 (HP)	0x174 - 0x175 (HM)	0x176 - 0x177 (EXP)	0x178 (EXP)

Char 13	0x18E (STR)	0x18F (INT)	0x190 (DEX)	0x191 (MAG)	0x192 - 0x193 (HP)	0x194 - 0x195 (HM)	0x196 - 0x197 (EXP)	0x198 (EXP)
Char 14	0x1AE (STR)	0x1AF (INT)	0x1B0 (DEX)	0x1B1 (MAG)	0x1B2 - 0x1B3 (HP)	0x1B4 - 0x1B5 (HM)	0x1B6 - 0x1B7 (EXP)	0x1B8 (EXP)
Char 15	0x1CE (STR)	0x1CF (INT)	0x1D0 (DEX)	0x1D1 (MAG)	0x1D2 - 0x1D3 (HP)	0x1D4 - 0x1D5 (HM)	0x1D6 - 0x1D7 (EXP)	0x1D8 (EXP)
Char 16	0x1EE (STR)	0x1EF (INT)	0x1F0 (DEX)	0x1F1 (MAG)	0x1F2 - 0x1F3 (HP)	0x1F4 - 0x1F5 (HM)	0x1F6 - 0x1F7 (EXP)	0x1F8 (EXP)
Food	0x202 - 0x203							
Gold	0x204 - 0x205							
Keys	0x206							
Gems	0x207							
MagCar	0x20A							
SkKeys	0x20B							
BlBadg	0x218							
MagAx	0x240							