Keira Wong
Prof. A Giacalone
CECS 378-01
November 8, 2020

Lab 2: Malware

I. Write-up / Experience

A. I downloaded the recommended binary hex editor and opened the files that I thought would most likely contain key information. Most files' names were the names of locations or castles I found on the game's map or small features of the game and most of these files ended in .OVL, .BIT, or a few numbers. I considered editing Z-STATS.OVL but could not find any meaningful patterns when opened in the binary hex editor and I remembered that was just a command in the game. After these conclusions, I ended up reviewing the INIT.GAM and SAVED.GAM seeing as they were the only two files with the .GAM ending and both files had all sixteen character names listed in the decoded text. INIT.GAM made the most sense to edit so that every time someone created a character or initialized a new game they could start with their own stats, however, once I changed certain offsets, they did not seem to save. I then tried making edits in SAVED.GAM which did end up saving once I restarted the game. The number of bytes after each name matched the number of bytes after other names and the pattern of each character's corresponding bytes seemed similar. "AG," for example, stood out to me because each character had a letter followed by G which I originally thought represented a character's health but later found to be the character's type (ie. "Avatar") upon analyzing the z-stats of my character. After more thought, I ended up using a programming calculator to translate back and forth between each byte's hex-value and each decimal value listed under the z-stats of each character in the game to determine what bytes each z-stat corresponded to. For other attributes like items, I ended up applying the same method by reviewing the z-stats' item and equipment window and translating each number listed for an item to its hex-value and searching the binary file for that hex-value and changing them along the way by trial-and-error.

II. Files & the Offsets Modified (in Hex Format)

A. "SAVED.GAM" file:

1. Characters (each 32-bytes)

CHARACTERS	**ADDRESS/OFFSET**
KEIRA	0x00000000

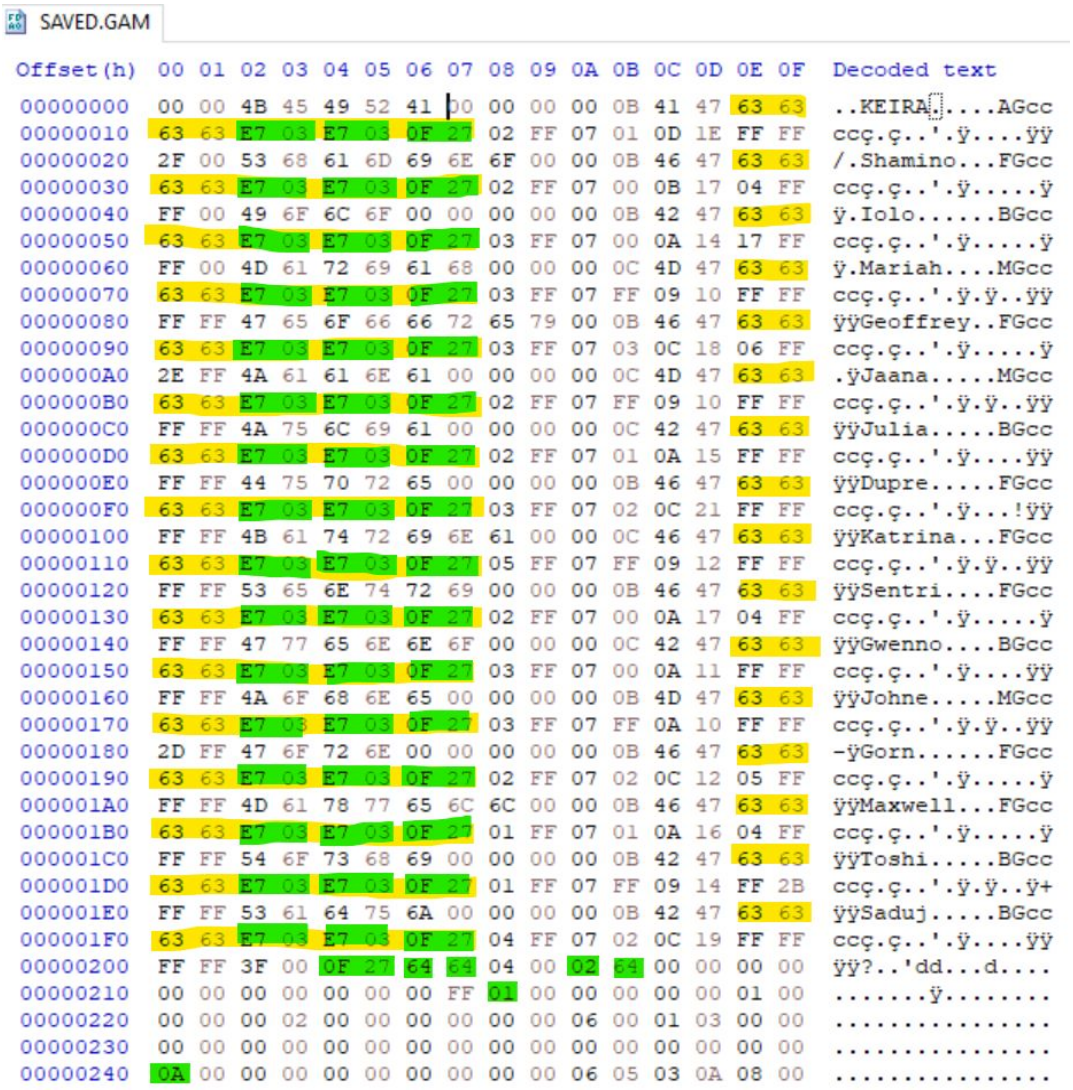
Shamino	0x00000020
Iolo	0x00000040
Mariah	0x00000060
Geoffrey	0x00000080
Jaana	0x000000A0
Julia	0x000000C0
Dupre	0x000000E0
Katrina	0x00000100
Sentri	0x00000120
Gweno	0x00000140
Johne	0x00000160
Gorn	0x00000180
Maxwell	0x000001A0
Toshi	0x000001C0
Saduj	0x000001E0

2. Stats (each 1- or 2-bytes)

Char's STATS	**ADDRESS/OFFSET**	**VALUE CHANGED TO (Big-Endian)**	**RESULT (dec)**
Strength	[Char's Offset] + 0x0000000E	0x00000063	99
Intelligence	[Char's Offset] + 0x0000000F	0x00000063	99
Dexterity	[Char's Offset] + 0x00000010	0x00000063	99
Magic	[Char's Offset] + 0x00000011	0x00000063	99
HP	[Char's Offset] + 0x00000012	0x000003E7	999
Max HP	[Char's Offset] + 0x00000014	0x000003E7	999
Experience	[Char's Offset] + 0x00000016	0x0000270F	9999

3. Items (each 1- or 2-bytes)

ITEMS	ADDRESS/OFFSET	VALUE CHANGED TO (Big-Endian)	RESULT (dec)
Gold	0x00000204	0x0000270F	9999
Keys	0x00000206	0x00000064	100
Skull Keys	0x0000020B	0x00000063	100
Gems	0x00000207	0x00000063	100
Black Badges	0x00000218	0x00000001	1
Magic Carpets	0x0000020A	0x00000002	2
Magic Axes	0x00000240	0x0000000A	10



III. Screenshots

A. Final Stats of My Main Character

(Str: 99; Int: 99; Dex: 99; HP: 999; Max HP: 999; Exp: 9999)

B. Final Stats for Party / Companion Characters

(Str: 99; Int: 99; Dex: 99; HP: 999; Max HP: 999; Exp: 9999)

C. Items

(100 Keys, 100 Skull Keys, 100 Gems, 1 Black Badge, 2 Magic Carpets, 10 Magic Axes)