

## 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

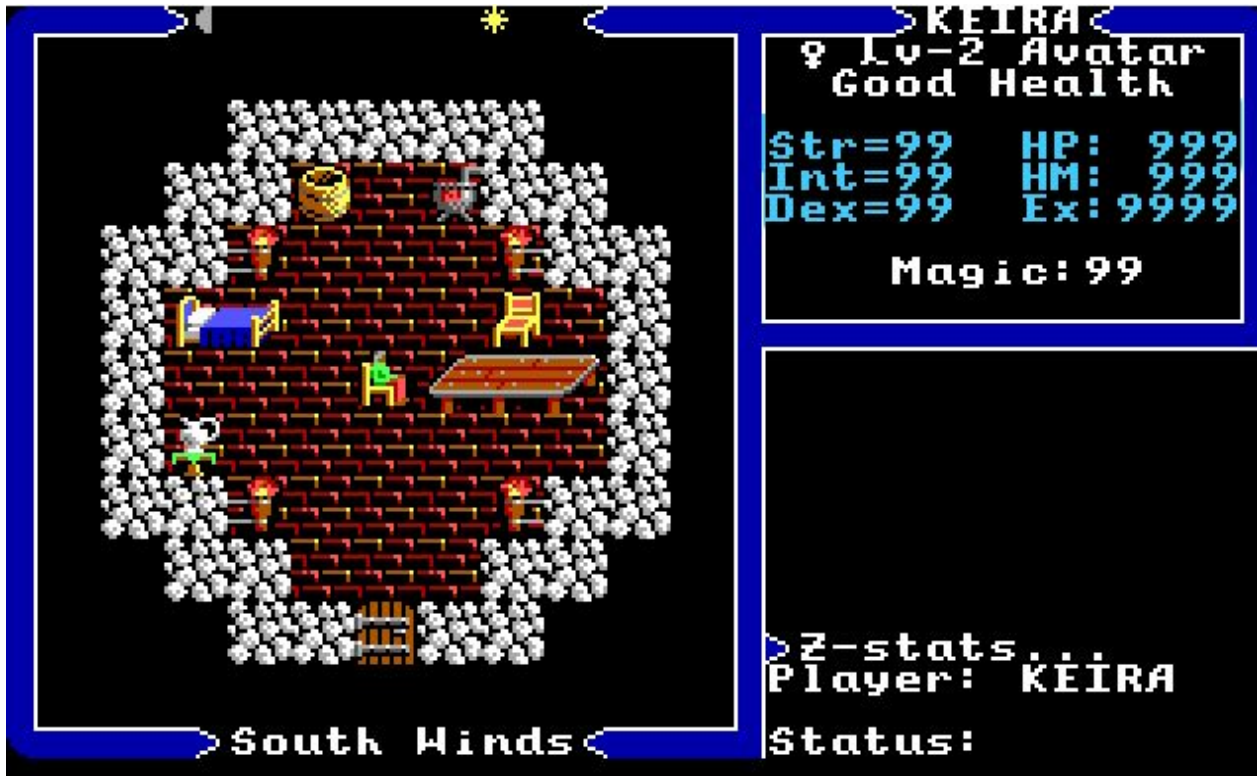

 The screenshot shows a memory editor window titled "SAVED.GAM". It displays a list of items with their corresponding memory addresses (Offset(h)) and values. The items are listed in a column on the left, and the values are shown in a grid of hex and decimal digits. The values are highlighted in yellow. The items are: Gold, Keys, Skull Keys, Gems, Black Badges, Magic Carpets, Magic Axes, and a series of other items. The values are: 0x0000270F, 0x00000064, 0x00000063, 0x00000063, 0x00000001, 0x00000002, 0x0000000A, and a series of other values.
 SAVED.GAM

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	00	00	4B	45	49	52	41	00	00	00	0B	41	47	63	63	..KEIRA....AGcc	
00000010	63	63	E7	03	E7	03	0F	27	02	FF	07	01	0D	1E	FF	FF	ccq.ç...'.ÿ....ÿÿ
00000020	2F	00	53	68	61	6D	69	6E	6F	00	00	0B	46	47	63	63	/.Shamino...FGcc
00000030	63	63	E7	03	E7	03	0F	27	02	FF	07	00	0B	17	04	FF	ccq.ç...'.ÿ....ÿ
00000040	FF	00	49	6F	6C	6F	00	00	00	00	00	0B	42	47	63	63	ÿ.Iolo.....BGcc
00000050	63	63	E7	03	E7	03	0F	27	03	FF	07	00	0A	14	17	FF	ccq.ç...'.ÿ....ÿ
00000060	FF	00	4D	61	72	69	61	68	00	00	00	0C	4D	47	63	63	ÿ.Mariah....MGcc
00000070	63	63	E7	03	E7	03	0F	27	03	FF	07	FF	09	10	FF	FF	ccq.ç...'.ÿ.ÿ..ÿÿ
00000080	FF	FF	47	65	6F	66	66	72	65	79	00	0B	46	47	63	63	ÿÿGeoffrey...FGcc
00000090	63	63	E7	03	E7	03	0F	27	03	FF	07	03	0C	18	06	FF	ccq.ç...'.ÿ....ÿ
000000A0	2E	FF	4A	61	61	6E	61	00	00	00	00	0C	4D	47	63	63	.ÿJaana.....MGcc
000000B0	63	63	E7	03	E7	03	0F	27	02	FF	07	FF	09	10	FF	FF	ccq.ç...'.ÿ.ÿ..ÿÿ
000000C0	FF	FF	4A	75	6C	69	61	00	00	00	00	0C	42	47	63	63	ÿÿJulia.....BGcc
000000D0	63	63	E7	03	E7	03	0F	27	02	FF	07	01	0A	15	FF	FF	ccq.ç...'.ÿ....ÿÿ
000000E0	FF	FF	44	75	70	72	65	00	00	00	00	0B	46	47	63	63	ÿÿDupre.....FGcc
000000F0	63	63	E7	03	E7	03	0F	27	03	FF	07	02	0C	21	FF	FF	ccq.ç...'.ÿ...!ÿÿ
00000100	FF	FF	4B	61	74	72	69	6E	61	00	00	0C	46	47	63	63	ÿÿKatrina...FGcc
00000110	63	63	E7	03	E7	03	0F	27	05	FF	07	FF	09	12	FF	FF	ccq.ç...'.ÿ.ÿ..ÿÿ
00000120	FF	FF	53	65	6E	74	72	69	00	00	00	0B	46	47	63	63	ÿÿSentri....FGcc
00000130	63	63	E7	03	E7	03	0F	27	02	FF	07	00	0A	17	04	FF	ccq.ç...'.ÿ....ÿ
00000140	FF	FF	47	77	65	6E	6E	6F	00	00	00	0C	42	47	63	63	ÿÿGwenno....BGcc
00000150	63	63	E7	03	E7	03	0F	27	03	FF	07	00	0A	11	FF	FF	ccq.ç...'.ÿ....ÿÿ
00000160	FF	FF	4A	6F	68	6E	65	00	00	00	00	0B	4D	47	63	63	ÿÿJohne....MGcc
00000170	63	63	E7	03	E7	03	0F	27	03	FF	07	FF	0A	10	FF	FF	ccq.ç...'.ÿ.ÿ..ÿÿ
00000180	2D	FF	47	6F	72	6E	00	00	00	00	00	0B	46	47	63	63	-ÿGorn.....FGcc
00000190	63	63	E7	03	E7	03	0F	27	02	FF	07	02	0C	12	05	FF	ccq.ç...'.ÿ....ÿ
000001A0	FF	FF	4D	61	78	77	65	6C	6C	00	00	0B	46	47	63	63	ÿÿMaxwell...FGcc
000001B0	63	63	E7	03	E7	03	0F	27	01	FF	07	01	0A	16	04	FF	ccq.ç...'.ÿ....ÿ
000001C0	FF	FF	54	6F	73	68	69	00	00	00	00	0B	42	47	63	63	ÿÿToshi....BGcc
000001D0	63	63	E7	03	E7	03	0F	27	01	FF	07	FF	09	14	FF	2B	ccq.ç...'.ÿ.ÿ..ÿ+
000001E0	FF	FF	53	61	64	75	6A	00	00	00	00	0B	42	47	63	63	ÿÿSaduj....BGcc
000001F0	63	63	E7	03	E7	03	0F	27	04	FF	07	02	0C	19	FF	FF	ccq.ç...'.ÿ....ÿÿ
00000200	FF	FF	3F	00	0F	27	64	64	04	00	02	64	00	00	00	00	ÿÿ?...'.dd....d....
00000210	00	00	00	00	00	00	00	FF	01	00	00	00	00	00	01	00	.....ÿ.....
00000220	00	00	00	02	00	00	00	00	00	00	06	00	01	03	00	00	.....ÿ.....
00000230	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....ÿ.....
00000240	0A	00	00	00	00	00	00	00	00	06	05	03	0A	08	00	00	.....ÿ.....

### 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)



KEIRA 999G  
Skamino 999G  
Iolo 999G

F: 63 G: 9999  
4-5-139

> Z-stats...  
Player: KEIRA  
Status: Done

South Winds



> Skamino <  
♂ Lv-2 Fighter  
Good Health

Str=99 HP: 999  
Int=99 HM: 999  
Dex=99 Ex: 9999

Magic: 99

> Z-stats...  
Player: KEIRA  
Status: ⚡

North Winds



> Iolo <  
♂ Lv-3 Bard  
Good Health

Str=99 HP: 999  
Int=99 HM: 999  
Dex=99 Ex: 9999

Magic: 99

> Z-stats...  
Player: KEIRA  
Status: ⚡

West Winds

### C. Items

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



North Winds

Equipment

Food: 63  
Gold: 9999

Keys.....100  
Gems.....100  
Torches.... 0

>Search-East  
Player: KEIRA  
Thou dost find  
nothing of note.

>East  
Blocked!

>Z-stats...  
Player: KEIRA  
Status:



East Winds

Items

2-B - 14  
3-I - Yellow  
1-A - Red  
2-Magic Crpt  
100-Skull Keys  
Pocket Watch 1  
1-Black Badge

>Search-East  
Player: KEIRA  
Thou dost find  
nothing of note.

>East  
Blocked!

>Z-stats...  
Player: KEIRA  
Status:



North Winds

Armaments

1-Sm. Shield  
2-Cloth  
1-Leather  
6-Dagger  
1-Club  
3-Flame Oil  
10-Magic Axe

↓

>Search-East  
Player: KEIRA  
Thou dost find  
nothing of note.

>East  
Blocked!

>Z-stats...  
Player: KEIRA  
Status: