

Ultima_5 Write Up

Monday, March 5, 2018

4:12 PM

Use CTL-E to exit from game to DOS

1. INIT.GAM has all the character names from start
2. BRIT.OOL was wiped after:
 - a. Torch item use
 - b. Save game
3. SAVED.GAM changes after:
 - a. Making a full new character and returning to the start menu
 - b. Pressing 'Q' in game

Offset	Hex	ASCII
0000	5363 6F74 7400 0000 000B 4647 0000 6363 E703 E703 0F27 02FF 0701 0D1E FFFF	Scott FG cc. . ' . ..
0032	2F00 5368 616D 696E 6F00 000B 4647 1416 1000 0500 3C00 A700 02FF 0700 0B17 04FF	/ Shamino FG < . . .
0064	FF00 496F 6C6F 0000 0000 000B 4247 1315 1108 5A00 5A00 F900 03FF 0700 0A14 17FF	. Iolo BG Z Z . . .
0096	FF00 4D61 7269 6168 0000 000C 4D47 0C14 1616 0200 5A00 1601 03FF 07FF 0910 FFFF	. Mariah MG Z . . .
0128	FFFF 4765 6F66 6672 6579 000B 4647 1815 1000 5A00 5A00 0401 03FF 0703 0C18 06FF	..Geoffrey FG Z Z . . .
0160	2EFF 4A61 616E 6100 0000 000C 4D47 0F11 1515 3C00 3C00 8E00 02FF 07FF 0910 FFFF	..Jaana MG < < . . .
0192	FFFF 4A75 6C69 6100 0000 000C 4247 1513 1209 3C00 3C00 8A00 02FF 0701 0A15 FFFF	..Julia BG < < . . .
0224	FFFF 4475 7072 6500 0000 000B 4647 1612 1000 5A00 5A00 0C01 03FF 0702 0C21 FFFF	..Dupre FG Z Z . !..
0256	FFFF 4861 7472 696E 6100 000C 4647 1615 1200 9600 9600 2003 05FF 07FF 0912 FFFF	..Katrina FG
0288	FFFF 5365 6E74 7269 0000 000B 4647 1714 1300 3C00 3C00 6500 02FF 0700 0A17 04FF	..Senti FG < < e . .
0320	FFFF 4777 656E 6E6F 0000 000C 4247 1116 1108 5A00 5A00 EA00 03FF 0700 0A11 FFFF	..Gwenno BG Z Z . . .
0352	FFFF 4A6F 686E 6500 0000 000B 4D47 0E14 1818 5A00 5A00 CE00 03FF 07FF 0A10 FFFF	..Johnne MG Z Z . . .
0384	2DFF 476F 726E 0000 0000 000B 4647 1513 0F00 3C00 3C00 8600 02FF 0702 0C12 05FF	..Gorn FG < < . . .
0416	FFFF 4D61 7877 656C 6C00 000B 4647 1513 0E00 1E00 1E00 2A00 01FF 0701 0A16 04FF	..Maxwell FG * . . .
0448	FFFF 546F 7368 6900 0000 000B 4247 1115 1008 1E00 1E00 4000 01FF 07FF 0914 FF2B	..Toshi BG @ . . .+
0480	FFFF 5361 6475 6A00 0000 000B 4247 151A 140A 7800 7800 1D02 04FF 0702 0C19 FFFF	..Saduj BG x x . . .
0512	FFFF 3F00 0F27 0200 0300 0000 0000 0000 0000 0000 0000 00FF 0000 0000 0100	..? ' .
0544	0000 0002 0000 0000 0000 0600 0103 0000 0000 0000 0000 0000 0000 0000 0000	
0576	0000 0000 0000 0000 0000 0605 030A 0800 0004 0000 0000 0202 0000 0000 0000	
0608	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0200 0000	
0640	0000 0003 0000 0000 0000 E060 2632 A668 17B8 8566 E025 13C2 7EA7 0000 0000 0000	..&2.h ..f.% ~.
0672	0000 0000 0000 0000 0000 0406 0706 0003 0000 0000 0003 0000 0000 0000 0000	
0704	0000 0000 0000 0000 0000 0000 8800 0000 0000 0000 1C04 0508 0829 0000 0032	.) 2
0736	3300 4800 0006 0000 0000 0001 020D 0000 0F0F 0000 0000 0000 0001 0000 0132	3 K 2
0768	00EC 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000	.
0800	0000 0000 00FF 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000	.
0832	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000	
0864	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000	
0896	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000	
0928	0000 0000 0000 0000 0000 0000 0000 0000 0000 FF01 0000 0000 0000 0000 0000	.
0960	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000	
0992	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000	

For this picture: Byte Offsets

2/3: represent beginning of the name

4/5/6/7: Name

8/9/10: Name

0xB: has 0B or 0C for some reason (probably some terminator)

12/13: Character class
14: Strength (63)
15: Dexterity (63)
16: Intelligence (63)
17: Magic (63)
18: HP1 (E7)
19: HP2 (03)
20: HM1 (E7)
21: HM2 (03)
22: EXP1 (0F)
23: EXP2 (27)
516: Gold1 (0F)
517: Gold (27)

For calculating hp... I entered 63633C on the internet and compared it to 63633C for Ultima_5

The image shows a web search result for '633c hex to decimal'. The search engine is DuckDuckGo. The result shows '25404' as the decimal equivalent of the hex value 633C. Below the result, there are filters for 'All Regions', 'Safe Search: Strict', and 'Any Time'. In the foreground, there is a screenshot of the Ultima 5 character selection screen. The screen shows a list of characters: Scott, Shamino, and Iolo. Scott's health points are shown as +25443G. The text 'cycles, Frameskip 0, Program: ULTIMA' is visible at the top of the screenshot. To the right of the screenshot, there is a watermark for 'binaryhexconverter.com' and a description of the website's purpose: 'to calculate decimal value from a hex number on table. to-decimal-converter'.

The system is big endian: (check in the health point bytes to confirm)
6300 is 99 (base 10)
0063 is 25344 (base 10)

E703 is 999 (base 10)

Python Malware Attempt:

To simplify the file manipulation, I kept a Clean and Manip version of Ultima_5.

Script Methods:

- **isIdenticalFiles():** The script detects when files have changed by comparing the Clean and Manip directories. This was the script I used to find the changed files when I messed with the saves. The only important file that we need to manipulate is the **SAVED.GAM**
- **openTempFile():** If you want to work off a temporary file in the manipulated folder, this allows you to open the SAVED.GAM file and create a temporary files.
- **modMainCharacterStats(decList):** This works directly with the Main Character's offsets to manipulate the decimal values provided by decList.
- **modSaveState():** Opens, reads, manipulates, writes and closes the SAVED.GAM file. This is the method used when running the program. Mocks a "Main" method.

Shell Attempt:

My idea of a traditional malware uses the computer's shell commands to run the program without having to use input/output readers.

I went through the shell commands with you and they worked in MacOS terminal. When I tried to run the commands through a Python script, the files would not change when I would write a new file.

I/O Finish:

I took the easy way out and read the file through a simple file open. The hard part was converting the file to a mutable format. I chose decimal because the values are converted to decimal when you append the bytes to a list.

Then, to write the files back, you need to change a decimal list to a byte array. You can use `bytes(list)` to do this.