Lorenzo Murillo IV
CECS 387 Sec 01

# Malware Lab Write-up

Determining the offsets with the hex editor was a bit odd at first, I went through a few files. After creating my character, I noticed that the file that was saved to was SAVED.GAM. As a result of this I decided to start changing some of the file contents. To create a basic test, I would insert five to ten “01” in random slots of the hex editor then run the game to see if I could notice any changes. After iterating through the file, I noticed there was a pattern when it came to the character information and the contents following their names. After collecting information regarding the file, I was able to take down all of the hex addresses as follows:

1) offset for Main Character starts: 0x0000 000E (14) ends: 0x0000 0015 (22)
2) offset for Shamito starts: 0x0000 002E (46) ends: 0x0000 0035 (54)
3) offset for Iolo starts: 0x0000 004E (78) ends: 0x0000 0055 (86)
4) offset for Mariah starts: 0x0000 006E (110) ends: 0x0000 0075 (118)
5) offset for Geoffrey starts: 0x0000 008E (142) ends: 0x0000 0095 (150)
6) offset for Jaana starts: 0x0000 00AE (174) ends: 0x0000 00B5 (182)
7) offset for Julia starts: 0x0000 00CE (206) ends: 0x0000 00D5 (214)
8) offset for Dupree starts: 0x0000 00E7 (238) ends: 0x0000 00EE (246)
9) offset for Katrina starts: 0x0000 010E (270) ends: 0x0000 0115 (278)
10) offset for Sentri starts: 0x0000 012E (302) ends: 0x0000 0135 (310)
11) offset for Gwenno starts: 0x0000 014E (334) ends: 0x0000 0155 (342)
12) offset for Johne starts: 0x0000 016E (366) ends: 0x0000 0175 (374)
13) offset for Gorn starts: 0x0000 018E (398) ends: 0x0000 0195 (406)
14) offset for Maxwell starts: 0x0000 01AE (430) ends: 0x0000 01B5 (438)
15) offset for Toshi starts: 0x0000 01CE (462) ends: 0x0000 01D5 (470)
16) offset for Saduj starts: 0x0000 01EE (494) ends: 0x0000 01F5 (502)

NOTE: For each character, to max out we use 63 63 63 63 E7 03 E7 03 0F 27in their respective modifiers: STR DEX INT HP MAX HP EXP respectively.

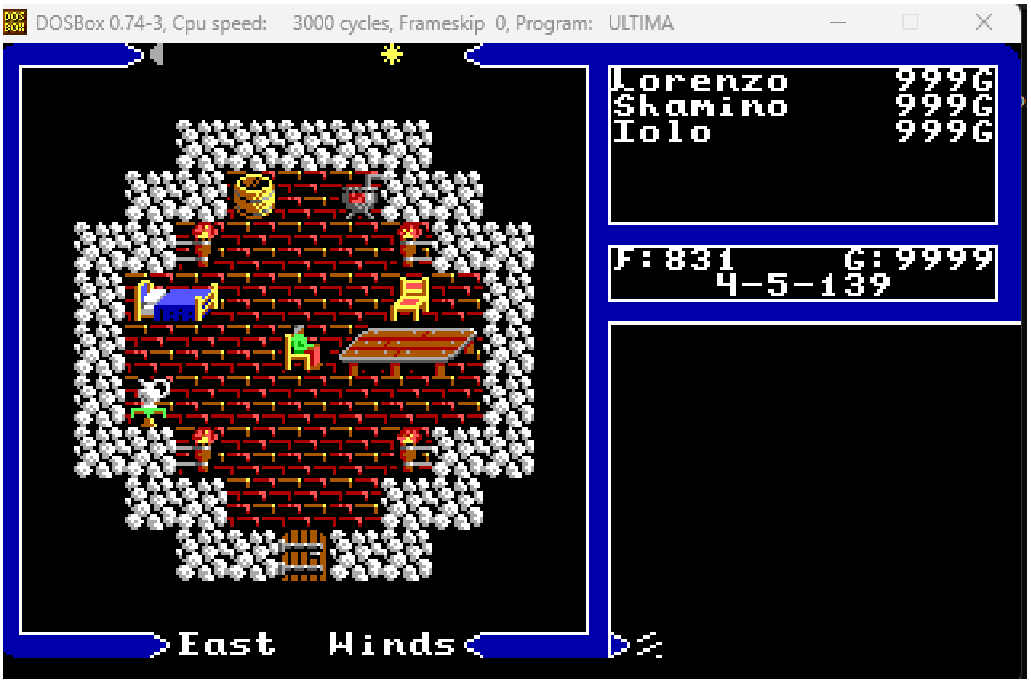
Also, the item hex offsets are as follows:

| | |
|---|---|
| Gold: | 0x00000204-5 |
| Keys: | 0X00000206 |
| Gems: | 0X00000207 |
| Torches: | 0X00000208 |
| Magic Carpets: | 0X0000020A |
| Skull Key: | 0X0000020B |
| Black Badge: | 0x00000218 |

| | |
|---|---|
| Magic Axes: | 0x00000240 |

After examining the file, I noticed that I could make a general equation that would allow me to access each character by calculating their offset.

Party Screencap:

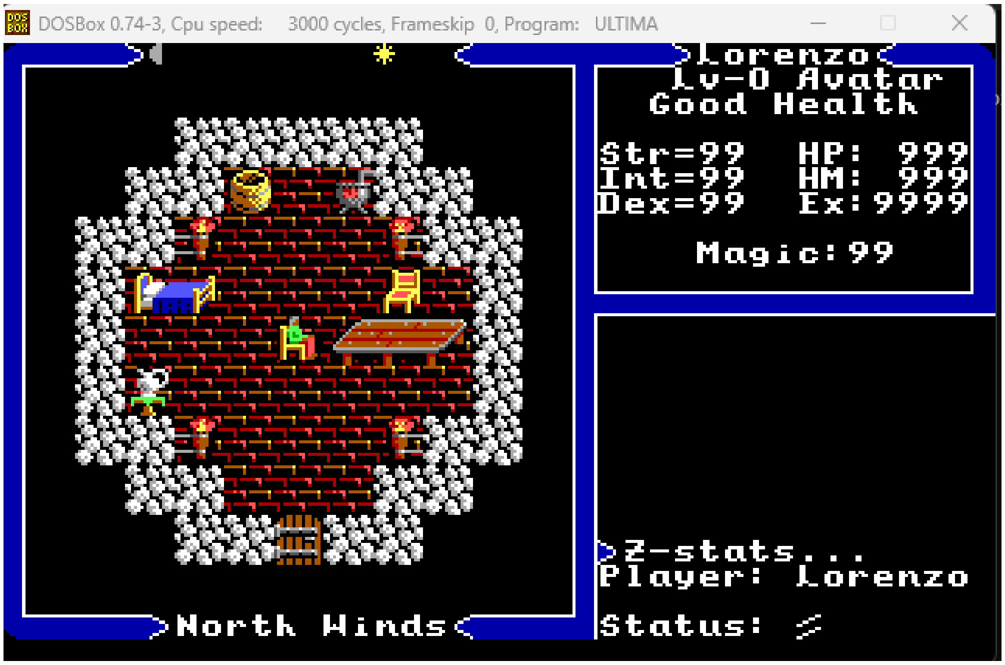

DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: ULTIMA

| | |
|---|---|
| Lorenzo | 999G |
| Shamino | 999G |
| Iolo | 999G |

F:831 G:9999
4-5-139

East Winds

Lorenzo Max Stats:


DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: ULTIMA

Lorenzo
Lv-0 Avatar
Good Health

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

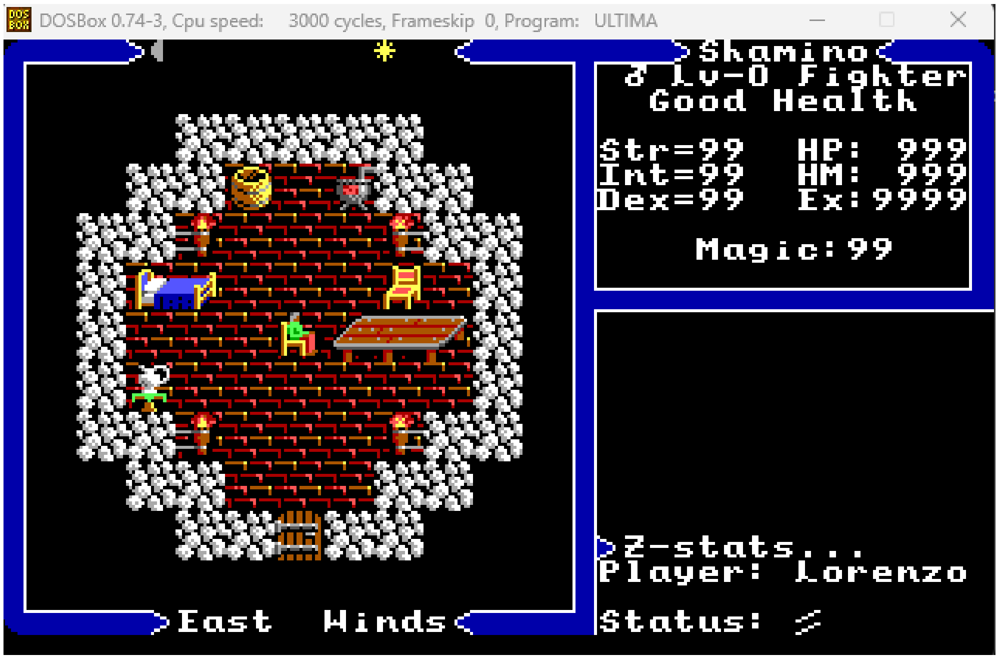
Magic:99

Z-stats...
Player: Lorenzo
Status:

North Winds

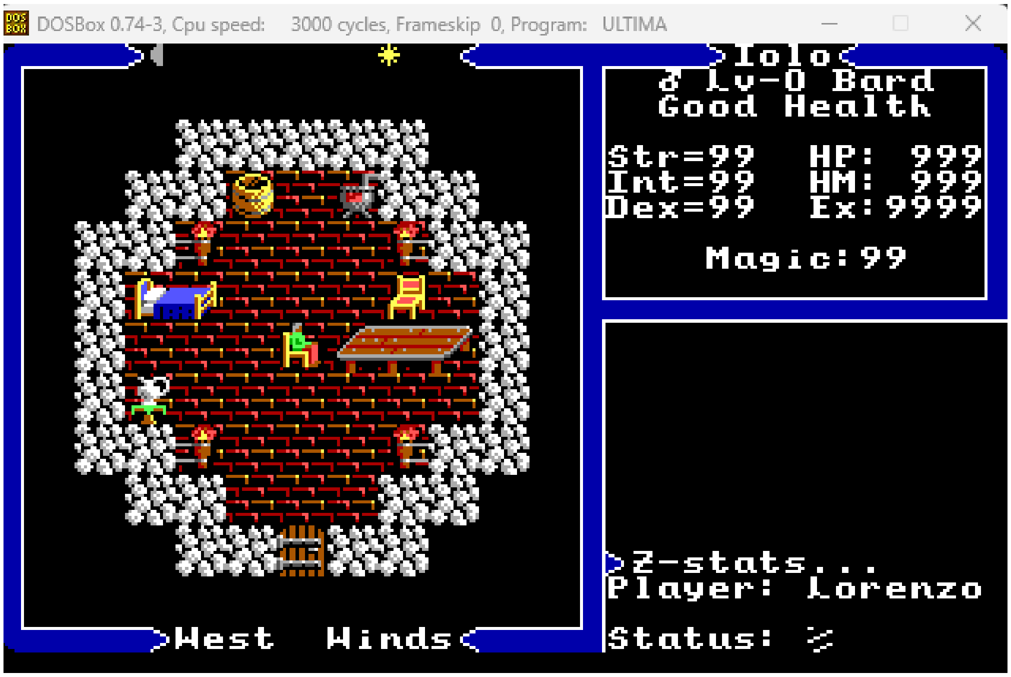
Lorenzo Murillo IV<br>
CECS 387 Sec 01

Shamino Max Stats:


DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: ULTIMA
East Winds

```
    Shamino
 ♂ Lv-0 Fighter
  Good Health

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

    Magic:99

>Z-stats...
Player: Lorenzo

Status: ⚡
```

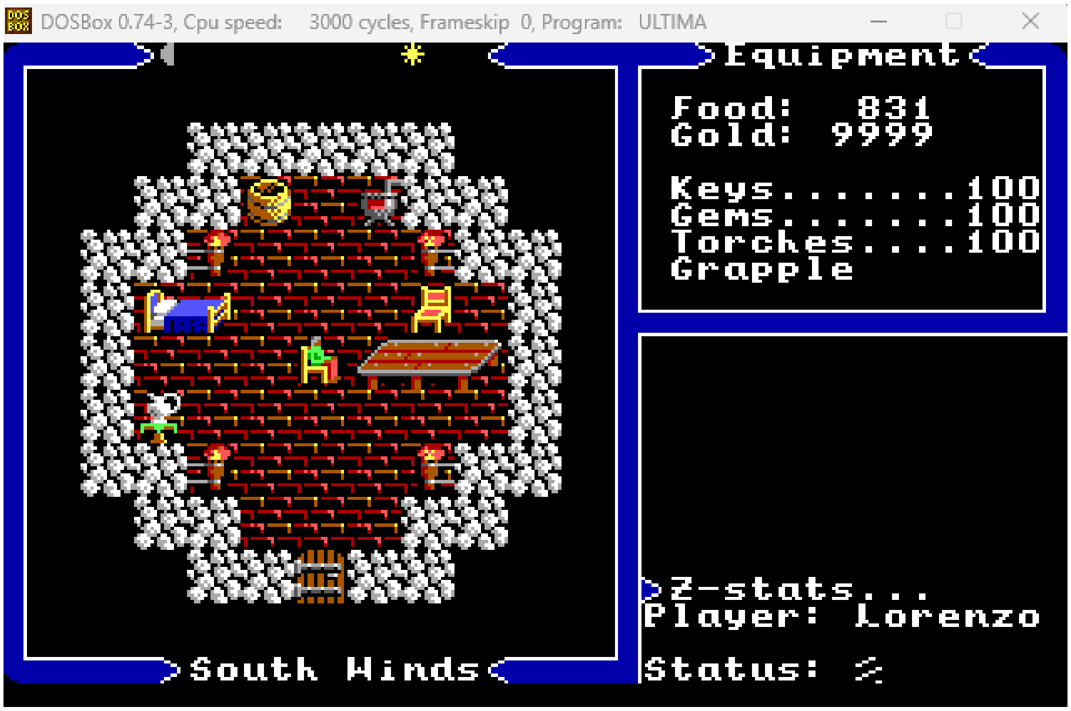
Iono Max Stats:


DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: ULTIMA
West Winds

```
      Iolo
  ♂ Lv-0 Bard
  Good Health

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

    Magic:99

>Z-stats...
Player: Lorenzo

Status: ⚡
```

Lorenzo Murillo IV
CECS 387 Sec 01

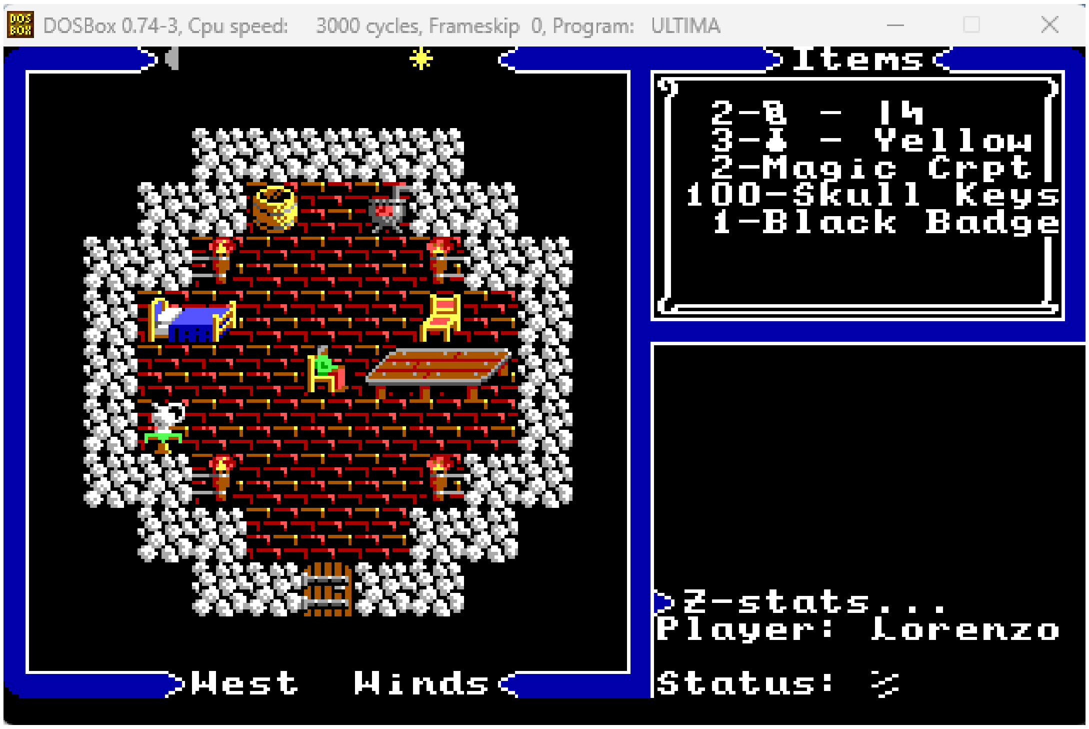
Keys Gems and Gold:



```
DOSBox 0.74-3, Cpu speed:     3000 cycles, Frameskip  0, Program:   ULTIMA
```

```
Equipment

Food:   831
Gold:  9999

Keys........100
Gems........100
Torches.....100
Grapple

>Z-stats...
Player: Lorenzo

South Winds                 Status: ≈
```

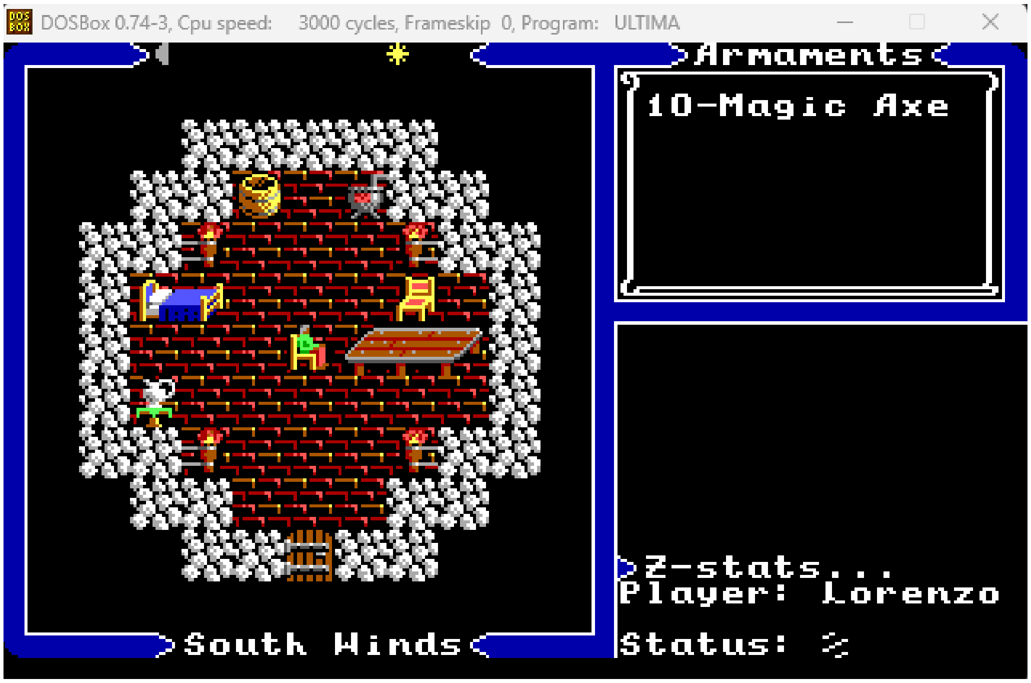
Magic Carpet, Skull Keys, and Black Badge:



```
DOSBox 0.74-3, Cpu speed:     3000 cycles, Frameskip  0, Program:   ULTIMA
```

```
Items

  2-▯ - I4
  3-♟ - Yellow
  2-Magic Crpt
100-Skull Keys
  1-Black Badge

>Z-stats...
Player: Lorenzo

West  Winds                 Status: ≈
```

Magic Axes:



DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: ULTIMA

```
Armaments
10-Magic Axe

Z-stats...
Player: Lorenzo
Status:
```

Finally, this file was saved in Little Endian, this meant we had to save our values in a particular way. For instance, if we were to have 999 in decimal the normal hex conversion is 03 E7, but when storing in the file we would use E7 03. In the case where values were ranging from 0-100, we did not have to adjust, only for larger values was it very important. Values like 100 in decimal would be converted to 64. If there was a location that required two elements the decimal value would be saved accordingly, like when changing EXP we would have 9999 -> 0F 27.