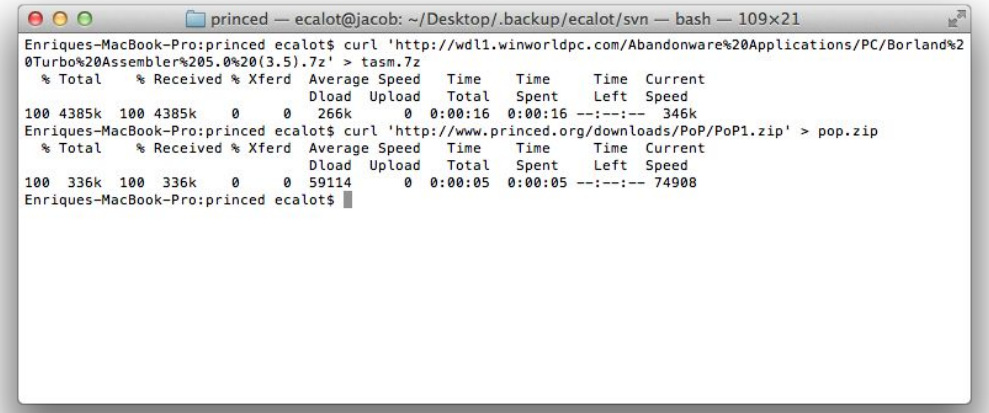
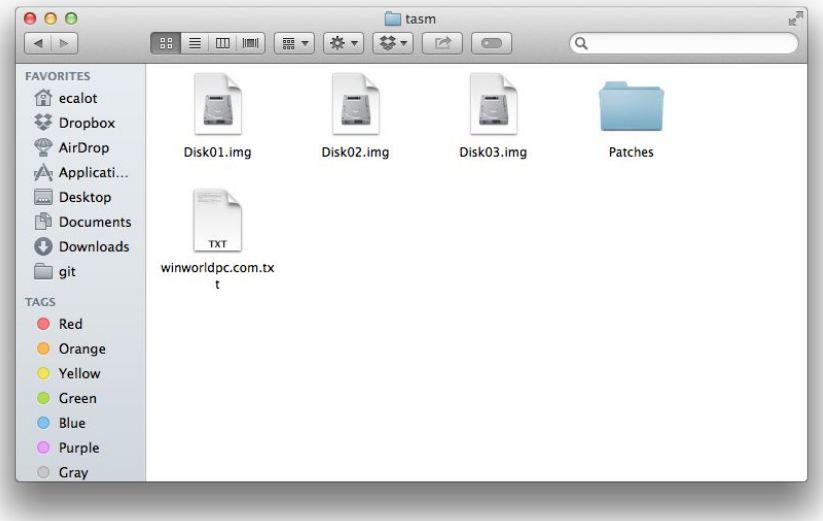
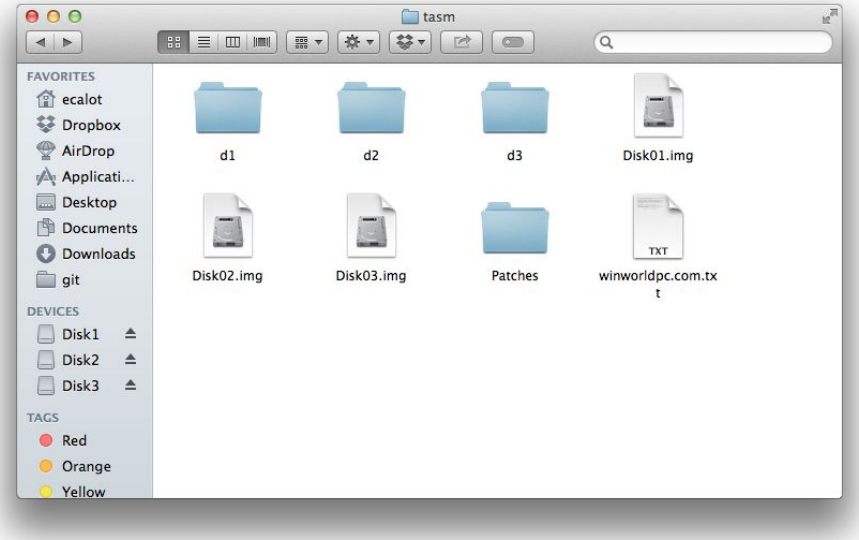
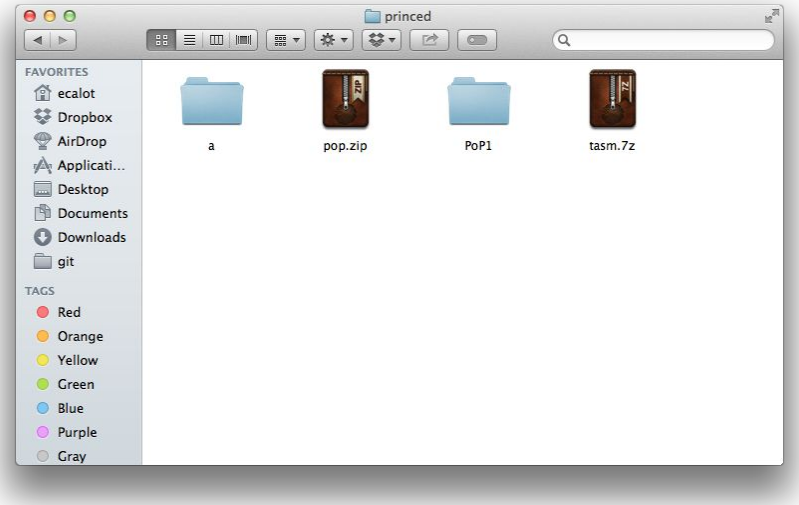
How to crack pop1 with CusAsm

First download pop1 and TASM package with TD in it.

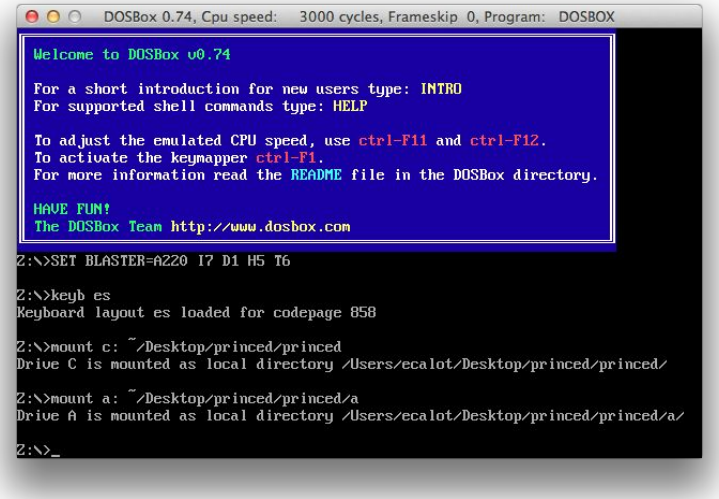




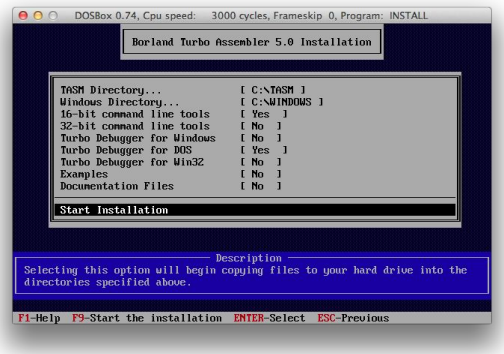


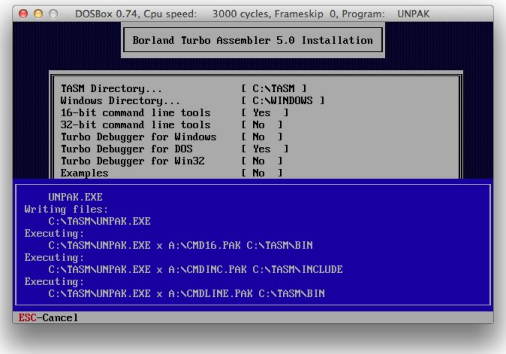


put all disk contents in a directory called “a” so you can mount it as a:

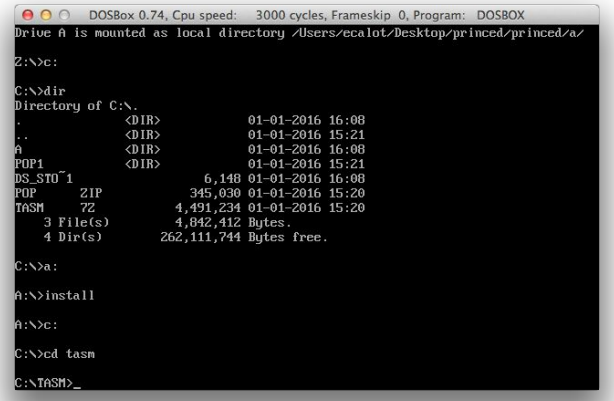


Only 16 bits version of TD is needed

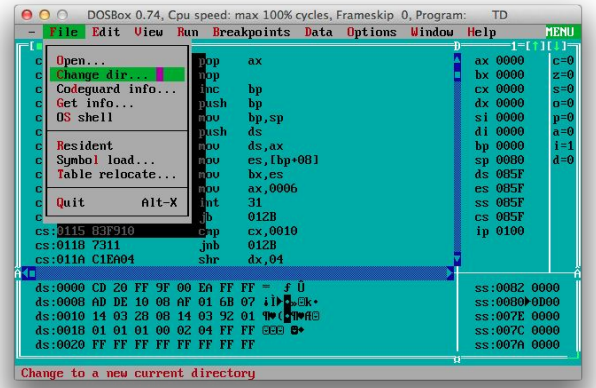


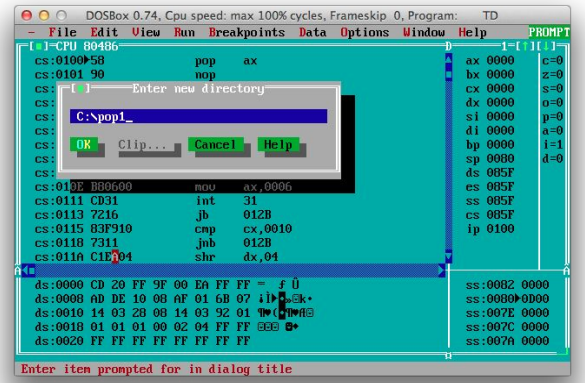


Inside TASM directory run TD in bin.

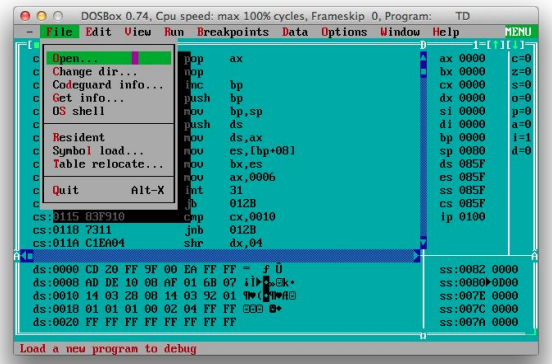


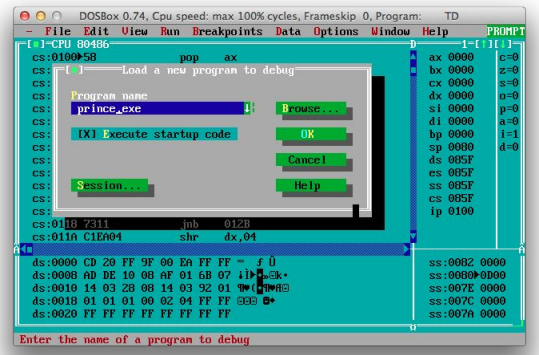
Then first set up the directory to pop1



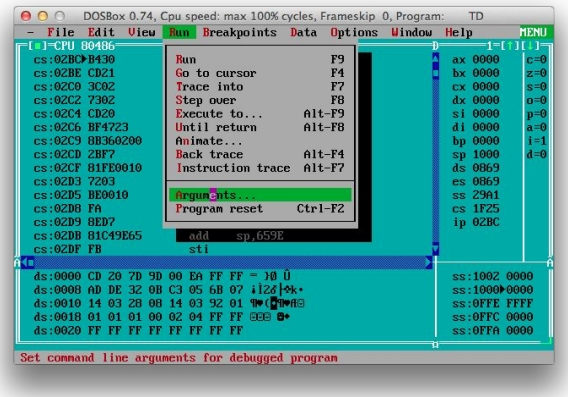


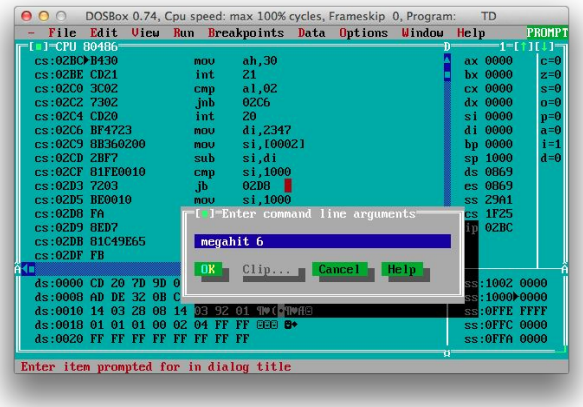
After that open prince.exe



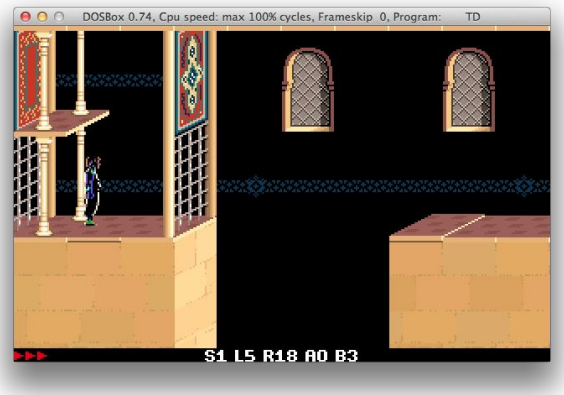


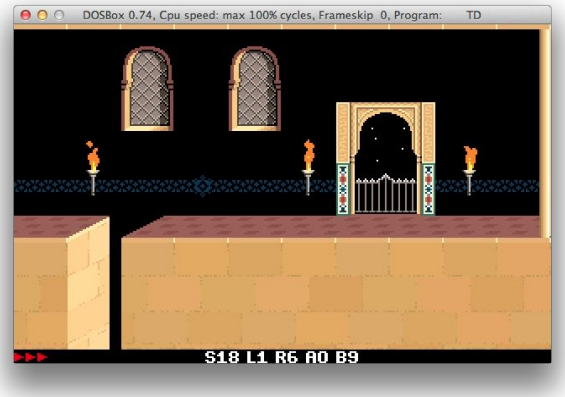
In this tutorial I'm going to move the shadow from level 6 to another screen, so I'll set up the parameters to "megahit 6" in order to debug faster





Now, with u,h,j,n it's possible to navigate the screens inside the game, with c the screen number is shown.





So we are moving the shadow from screen S1 (0x01) to S18 (0x12).

CODE: SELECT ALL

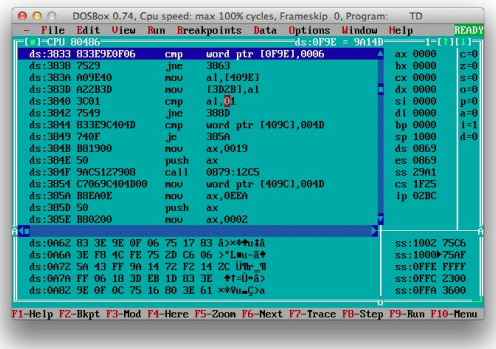
```
1109 833E9E0F0D      cmp    word ptr [0F9E],000D <-- level
1110 833E9E4017      cmp    word ptr [409E],0017 <-- room 1
1117 833E9E4010      cmp    word ptr [409E],0010 <-- room 2
112A C606ED4216      mov    byte ptr [42ED],16 <-- start tile
112F B8FF00          mov    ax,00FF
113A 250F00          and    ax,000F
1149 803EED421B      cmp    byte ptr [42ED],1B <-- end tile
```

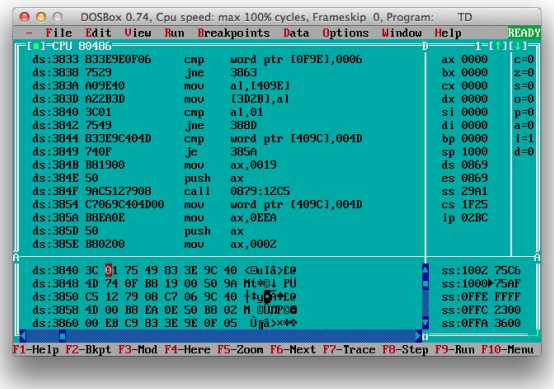
BBCode

Search for: 83 3e .. .. [b]0d[/b] 75 40 83 3e .. .. [b]17[/b] 74 07 83 3e .. .. [b]10[/b] 75 32 a1 .. .. a3 .. .. 50 .. .. c6 06 .. .. [b]16[/b] b8 [b]ff 00[/b] 50 9a .. .. 2a e4 25 [b]0f 00[/b] f7 d8 50 .. .. fe 06 .. .. 80 3e .. .. [b]1b[/b]
(offsets are p0:0x1209, u0:0x28b9, p3:0x13c4, u3:0x1b04, p4:0x1354, u4:0x2484)

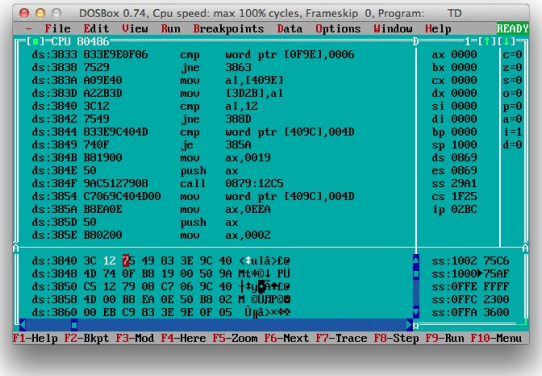
and replace
0d with
17 with
10 with
16 with
ff 00 with
0f 00 with
1b with

We know that in pop1.0 [0F9E] is the level and [409E] the current room. Other versions have other offsets but it is possible to find the corresponding offset of the version searching for the common code using the right wildcards.

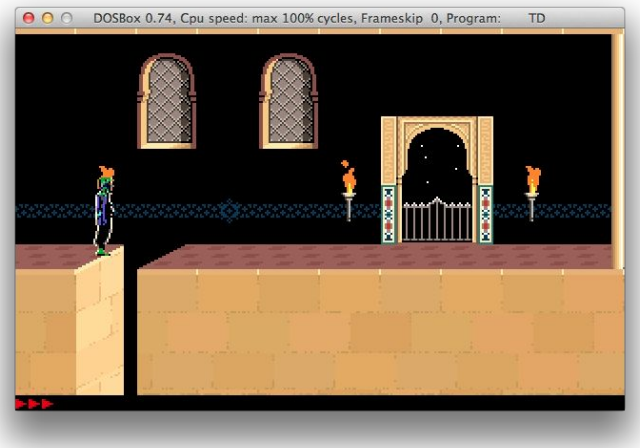




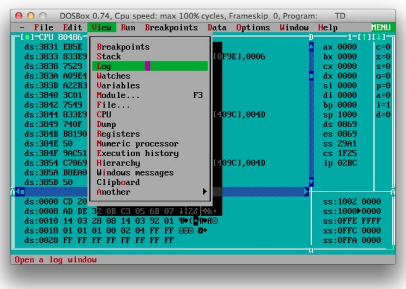
After finding a code where level 6 is compared and screen 1, I'm changing the byte 01 for 12 to test if this is the right place to edit the shadow guy position.

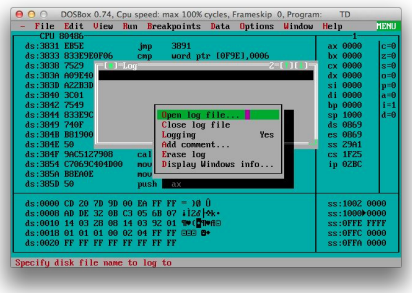


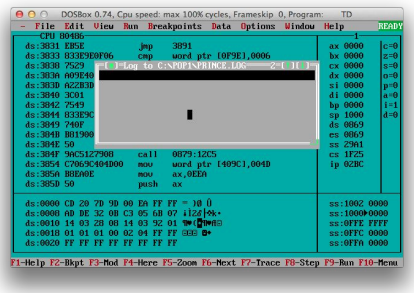
And finally on the first try, the shadow guy has been moved



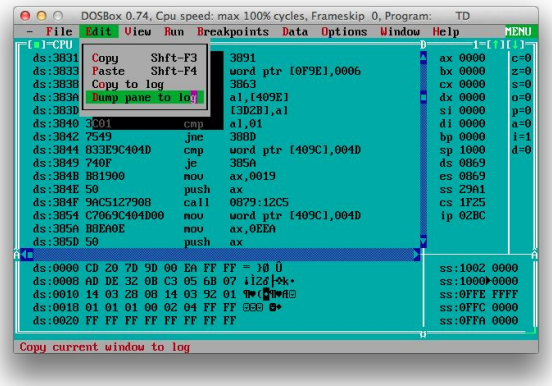
To copy the code, if you are in windows using cmd just copy the rectangle, if not, set up a log file



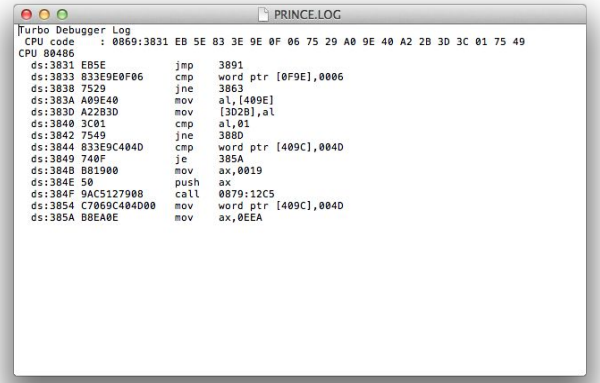


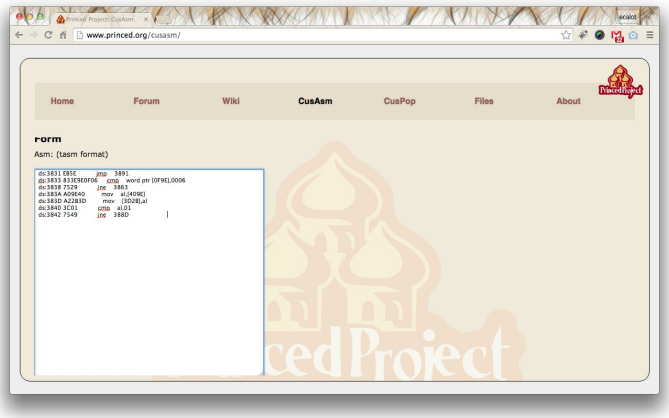


Then click on “dump pane to log”

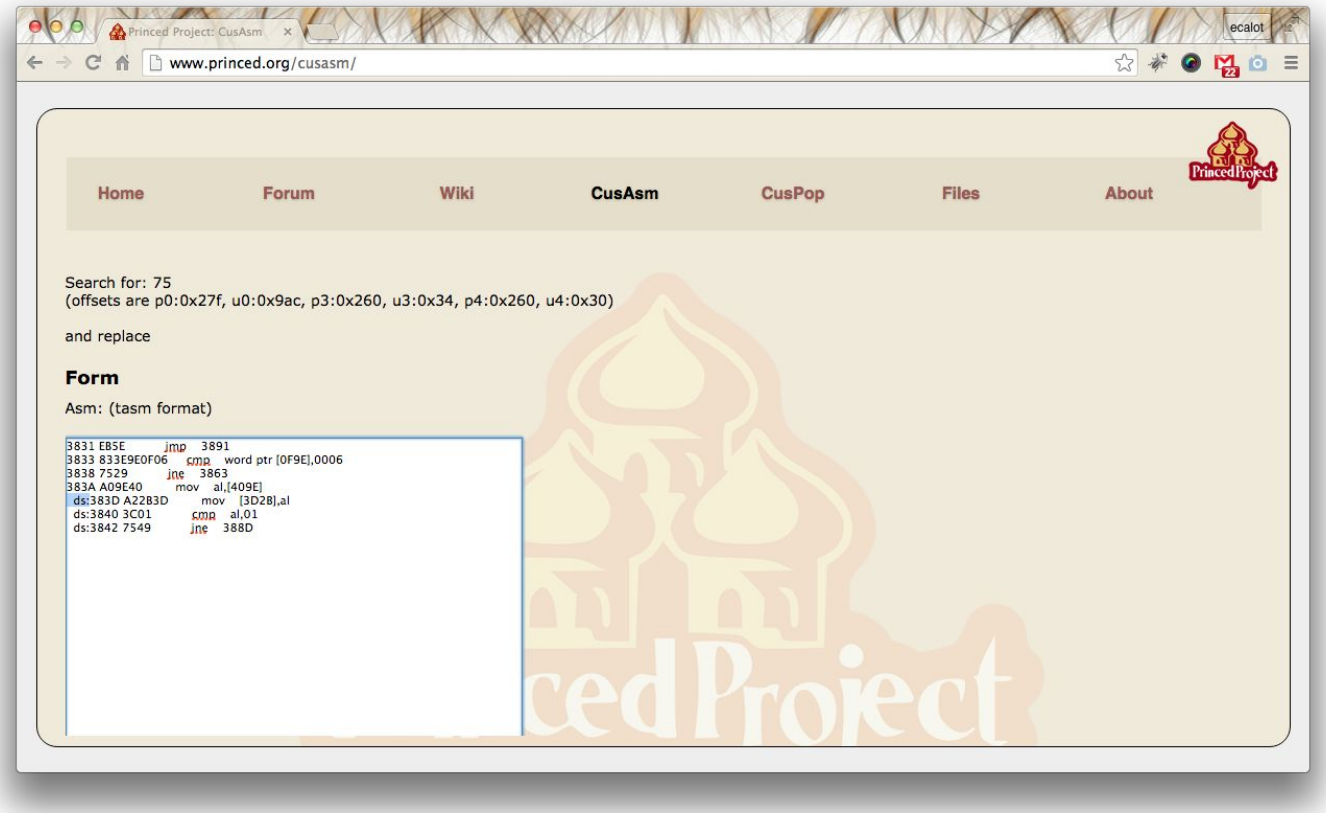


Copy the right lines from the file to cusasm





Finally, as CusAsm requires the first column to be 2 hex bytes (even though it is ignored), trim the beginning



And finally click on “get Code” (twice if possible to generate the mask and then the output).

Assembler

```
[code]
3831  eb 5e              jmp    3891
3833  83 3e 9e 0f 06     cmp    word ptr [0f9e],0006
3838  75 29              jne    3863
383a  a0 9e 40           mov    al,[409e]
383d  a2 2b 3d           mov    [3d2b],al
3840  3c 01              cmp    al,01
3842  75 49              jne    388d
[/code]
```

XML

```
<hack name="Hack name here">
        <offset file="p0" value="0x3931"/>
        <offset file="u0" value="0x4fe1"/>
        <offset file="p3" value="0x3db1"/>
        <offset file="u3" value="0x44f1"/>
        <offset file="p4" value="0x386d"/>
        <offset file="u4" value="0x499d"/>

        <check codes="eb 5e 83 3e .. .."/>
        <read default="06" name="name here" type=""/>
```