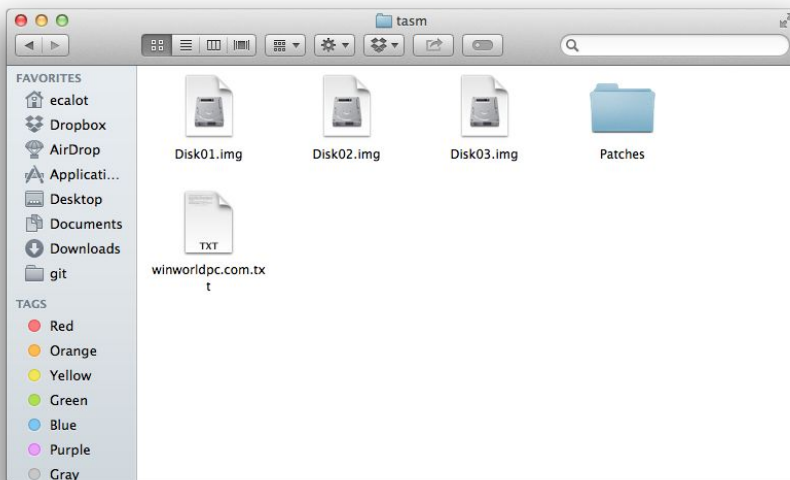
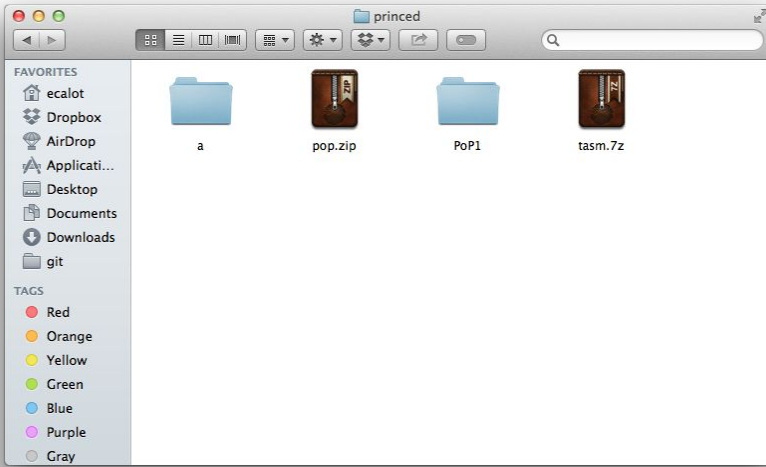
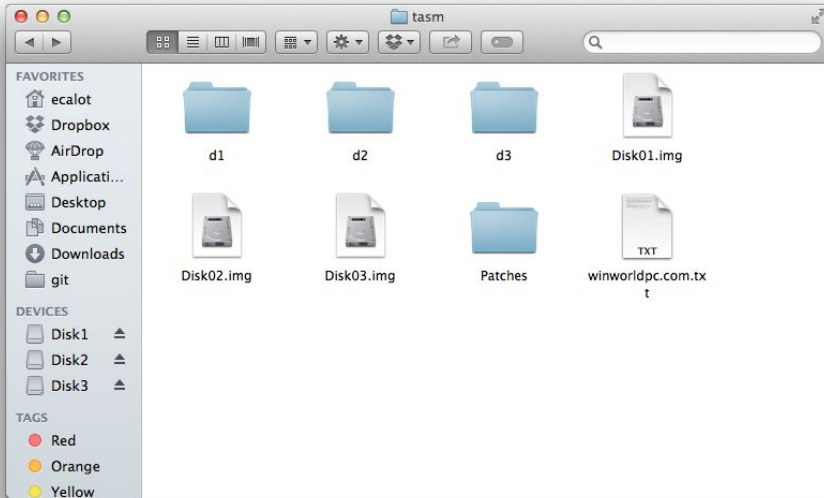


How to crack pop1 with CusAsm

First download pop1 and TASM package with TD in it.

```
Enriques-MacBook-Pro:princd ecalot$ curl 'http://wdl1.winworldpc.com/Abandonware%20Applications/PC/Borland%20Turbo%20Assembler%205.0%20(3.5).7z' > tasm.7z
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 4385k 100 4385k 0 0 266k 0 0:00:16 0:00:16 --:--:-- 346k
Enriques-MacBook-Pro:princd ecalot$ curl 'http://www.princd.org/downloads/PoP/PoP1.zip' > pop.zip
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 336k 100 336k 0 0 59114 0 0:00:05 0:00:05 --:--:-- 74908
Enriques-MacBook-Pro:princd ecalot$
```





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

```

DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX
Welcome to DOSBox v0.74
For a short introduction for new users type: INTRO
For supported shell commands type: HELP

To adjust the emulated CPU speed, use ctrl-F11 and ctrl-F12.
To activate the keymapper ctrl-F1.
For more information read the README file in the DOSBox directory.

HAVE FUN!
The DOSBox Team http://www.dosbox.com

Z:\>SET BLASTER=A220 I7 D1 H5 T6

Z:\>keyb es
Keyboard layout es loaded for codepage 858

Z:\>mount c: ~/Desktop/prnced/prnced
Drive C is mounted as local directory /Users/ecalot/Desktop/prnced/prnced/

Z:\>mount a: ~/Desktop/prnced/prnced/a
Drive A is mounted as local directory /Users/ecalot/Desktop/prnced/prnced/a/

Z:\>_

```

Only 16 bits version of TD is needed

```

DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: INSTALL
Borland Turbo Assembler 5.0 Installation

TASM Directory... [ C:\TASM ]
Windows Directory... [ C:\WINDOWS ]
16-bit command line tools [ Yes ]
32-bit command line tools [ No ]
Turbo Debugger for Windows [ No ]
Turbo Debugger for DOS [ Yes ]
Turbo Debugger for Win32 [ No ]
Examples [ No ]
Documentation Files [ No ]

Start Installation

Description
Selecting this option will begin copying files to your hard drive into the
directories specified above.

F1-Help F9-Start the installation ENTER-Select ESC-Previous

```

```

DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: UNPAK
Borland Turbo Assembler 5.0 Installation

TASM Directory... [ C:\TASM ]
Windows Directory... [ C:\WINDOWS ]
16-bit command line tools [ Yes ]
32-bit command line tools [ No ]
Turbo Debugger for Windows [ No ]
Turbo Debugger for DOS [ Yes ]
Turbo Debugger for Win32 [ No ]
Examples [ No ]

UNPAK.EXE
Writing files:
C:\TASM\UNPAK.EXE
Executing:
C:\TASM\UNPAK.EXE x A:\CMD16.PAK C:\TASM\BIN
Executing:
C:\TASM\UNPAK.EXE x A:\CMDINC.PAK C:\TASM\INCLUDE
Executing:
C:\TASM\UNPAK.EXE x A:\CMDLINE.PAK C:\TASM\BIN

ESC-Cancel

```

Inside TASM directory run TD in bin.

```

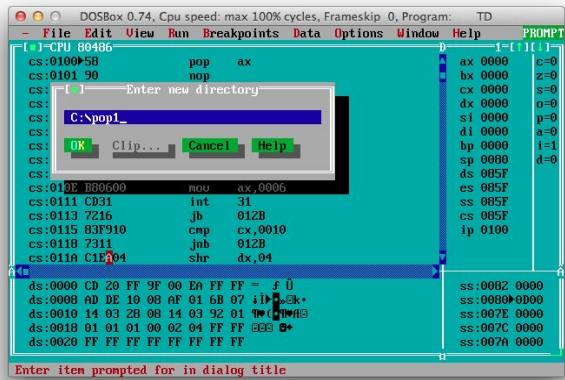
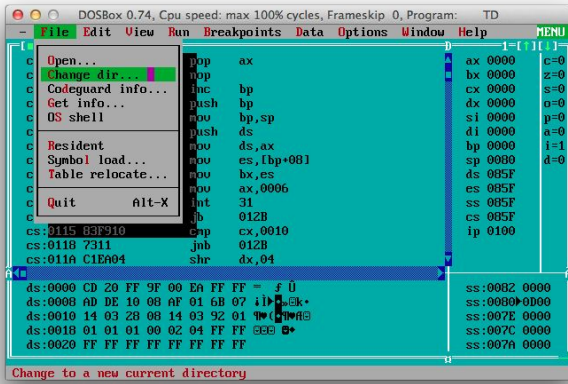
DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX
Drive A is mounted as local directory /Users/ecalot/Desktop/prnced/prnced/a/

Z:\>e:
C:\>dir
Directory of C:\
. <DIR> 01-01-2016 16:08
.. <DIR> 01-01-2016 15:21
A <DIR> 01-01-2016 16:08
POP1 <DIR> 01-01-2016 15:21
DS_ST01 6,148 01-01-2016 16:08
POP ZIP 345,030 01-01-2016 15:20
TASM 72 4,491,234 01-01-2016 15:20
3 File(s) 4,842,412 Bytes.
4 Dir(s) 262,111,744 Bytes free.

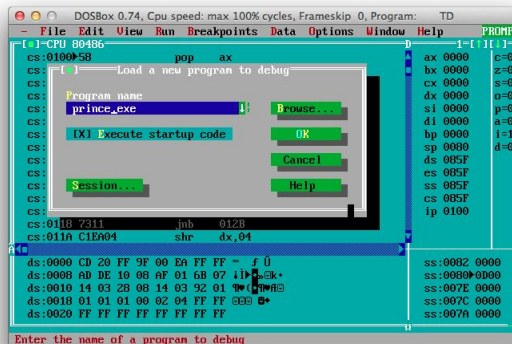
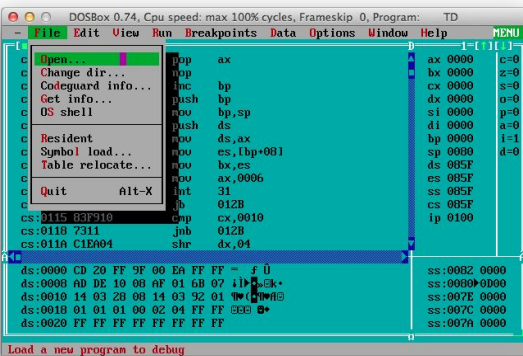
C:\>a:
A:\>install
A:\>e:
C:\>cd tasm
C:\TASM>_

```

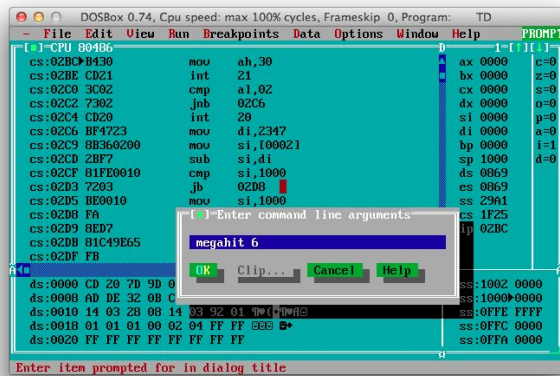
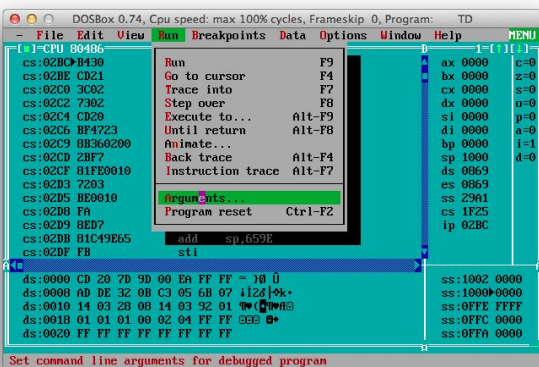
Then first set up the directory to pop1



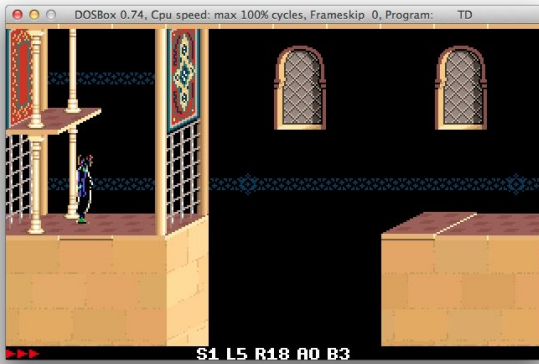
After that open prince.exe



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 C006ED4216    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
  
```

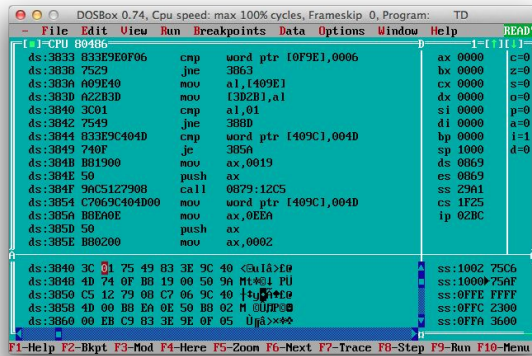
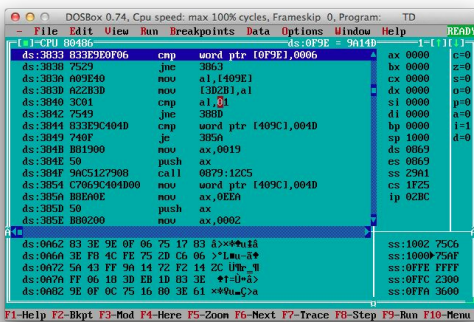
BBCode

```

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.

```

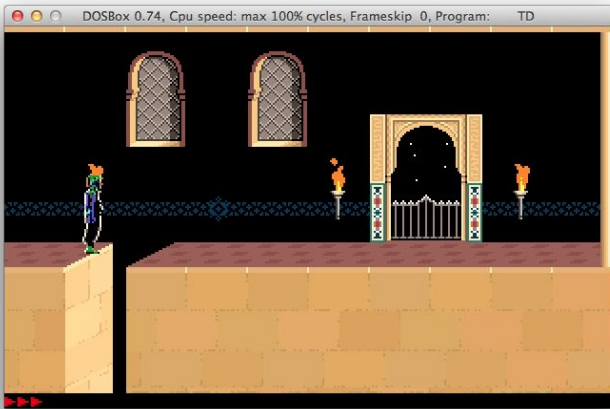
DOSBox 0.74, Cpu speed: max 100% cycles, Frameskip 0, Program: TD
- File Edit View Run Breakpoints Data Options Window Help
[=]-CPU 80486
ds:3833 E83E9E0F06 cmp word ptr [0F9E],0006 ax 0000 c=0
ds:3838 7529 jnc 3863 bx 0000 z=0
ds:383A A09E40 mov al,[409E] cx 0000 s=0
ds:383D A22E3D mov [3D2B],al dx 0000 o=0
ds:3840 9C12 cmp al,12 si 0000 p=0
ds:3842 7549 jnc 388D di 0000 a=0
ds:3844 E33E9C404D cmp word ptr [409C],004D bp 0000 i=1
ds:3849 740F jc 385A sp 1000 d=0
ds:384B B81900 mov ax,0019 ds 0869
ds:384E 50 push ax es 0869
ds:384F 9AC5127908 call 0879:12C5 ss 29A1
ds:3854 C7069C404D00 mov word ptr [409C],004D cs 1F25
ds:385A B8E40E mov ax,0E4A ip 02BC
ds:385D 50 push ax
ds:385E B80200 mov ax,0002

ds:0000 CD 20 7D 9D 00 E4 FF FF = 10 0
ds:0008 AD 32 0B C3 05 6B 07 1124
ds:0010 14 03 28 08 14 03 92 01
ds:0018 01 01 01 00 02 04 FF FF 800
ds:0020 FF FF FF FF FF FF FF FF

ds:1002 75C6
ds:1009 75AF
ds:0FFE FFFF
ds:0FFC 2300
ds:0FFA 3600

```

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

```

DOSBox 0.74, Cpu speed: max 100% cycles, Frameskip 0, Program: TD
- File Edit View Run Breakpoints Data Options Window Help
[=]-CPU 80486
Breakpoints
Stack
ds:3833 E83E9E0F06 cmp word ptr [0F9E],0006 ax 0000 c=0
ds:3838 7529 jnc 3863 bx 0000 z=0
ds:383A A09E40 mov al,[409E] cx 0000 s=0
ds:383D A22E3D mov [3D2B],al dx 0000 o=0
ds:3840 9C12 cmp al,12 si 0000 p=0
ds:3842 7549 jnc 388D di 0000 a=0
ds:3844 E33E9C404D cmp word ptr [409C],004D bp 0000 i=1
ds:3849 740F jc 385A sp 1000 d=0
ds:384B B81900 mov ax,0019 ds 0869
ds:384E 50 push ax es 0869
ds:384F 9AC5127908 call 0879:12C5 ss 29A1
ds:3854 C7069C404D00 mov word ptr [409C],004D cs 1F25
ds:385A B8E40E mov ax,0E4A ip 02BC
ds:385D 50 push ax
ds:385E B80200 mov ax,0002

ds:0000 CD 20 7D 9D 00 E4 FF FF = 10 0
ds:0008 AD 32 0B C3 05 6B 07 1124
ds:0010 14 03 28 08 14 03 92 01
ds:0018 01 01 01 00 02 04 FF FF 800
ds:0020 FF FF FF FF FF FF FF FF

ds:1002 75C6
ds:1009 75AF
ds:0FFE FFFF
ds:0FFC 2300
ds:0FFA 3600

```

```

DOSBox 0.74, Cpu speed: max 100% cycles, Frameskip 0, Program: TD
- File Edit View Run Breakpoints Data Options Window Help
[=]-CPU 80486
ds:3831 E83C jmp 3891 ax 0000 c=0
ds:3833 E83E9E0F06 cmp word ptr [0F9E],0006 bx 0000 z=0
ds:3838 7529 jnc 3863 cx 0000 s=0
ds:383A A09E40 mov al,[409E] dx 0000 o=0
ds:383D A22E3D mov [3D2B],al si 0000 p=0
ds:3840 9C12 cmp al,12 di 0000 a=0
ds:3842 7549 jnc 388D bp 0000 i=1
ds:3844 E33E9C404D cmp word ptr [409C],004D sp 1000 d=0
ds:3849 740F jc 385A ds 0869
ds:384B B81900 mov ax,0019 es 0869
ds:384E 50 push ax ss 29A1
ds:384F 9AC5127908 call 0879:12C5 cs 1F25
ds:3854 C7069C404D00 mov word ptr [409C],004D ip 02BC
ds:385A B8E40E mov ax,0E4A
ds:385D 50 push ax

ds:0000 CD 20 7D 9D 00 E4 FF FF = 10 0
ds:0008 AD 32 0B C3 05 6B 07 1124
ds:0010 14 03 28 08 14 03 92 01
ds:0018 01 01 01 00 02 04 FF FF 800
ds:0020 FF FF FF FF FF FF FF FF

ds:1002 75C6
ds:1009 75AF
ds:0FFE FFFF
ds:0FFC 2300
ds:0FFA 3600

```

```

DOSBox 0.74, Cpu speed: max 100% cycles, Frameskip 0, Program: TD
- File Edit View Run Breakpoints Data Options Window Help
[=]-CPU 80486
ds:3831 E83C jmp 3891 ax 0000 c=0
ds:3833 E83E9E0F06 cmp word ptr [0F9E],0006 bx 0000 z=0
ds:3838 7529 jnc 3863 cx 0000 s=0
ds:383A A09E40 mov al,[409E] dx 0000 o=0
ds:383D A22E3D mov [3D2B],al si 0000 p=0
ds:3840 9C12 cmp al,12 di 0000 a=0
ds:3842 7549 jnc 388D bp 0000 i=1
ds:3844 E33E9C404D cmp word ptr [409C],004D sp 1000 d=0
ds:3849 740F jc 385A ds 0869
ds:384B B81900 mov ax,0019 es 0869
ds:384E 50 push ax ss 29A1
ds:384F 9AC5127908 call 0879:12C5 cs 1F25
ds:3854 C7069C404D00 mov word ptr [409C],004D ip 02BC
ds:385A B8E40E mov ax,0E4A
ds:385D 50 push ax

ds:0000 CD 20 7D 9D 00 E4 FF FF = 10 0
ds:0008 AD 32 0B C3 05 6B 07 1124
ds:0010 14 03 28 08 14 03 92 01
ds:0018 01 01 01 00 02 04 FF FF 800
ds:0020 FF FF FF FF FF FF FF FF

ds:1002 75C6
ds:1009 75AF
ds:0FFE FFFF
ds:0FFC 2300
ds:0FFA 3600

```

Then click on "dump pane to log"

```

DOSBox 0.74, Cpu speed: max 100% cycles, Frameskip 0, Program: TD
- File Edit View Run Breakpoints Data Options Window Help
[=]-CPU 80486
Copy Shift-F3 3891 ax 0000 c=0
Paste Shift-F4 word ptr [0F9E],0006 bx 0000 z=0
Copy to log 3863 cx 0000 s=0
Jump pane to log al,[409E] dx 0000 o=0
ds:3833 E83E9E0F06 cmp word ptr [0F9E],0006 si 0000 p=0
ds:3838 7529 jnc 3863 di 0000 a=0
ds:383A A09E40 mov al,[409E] bp 0000 i=1
ds:383D A22E3D mov [3D2B],al sp 1000 d=0
ds:3840 9C12 cmp al,01 d1 0000 a=0
ds:3842 7549 jnc 388D bp 0000 i=1
ds:3844 E33E9C404D cmp word ptr [409C],004D sp 1000 d=0
ds:3849 740F jc 385A ds 0869
ds:384B B81900 mov ax,0019 es 0869
ds:384E 50 push ax ss 29A1
ds:384F 9AC5127908 call 0879:12C5 cs 1F25
ds:3854 C7069C404D00 mov word ptr [409C],004D ip 02BC
ds:385A B8E40E mov ax,0E4A
ds:385D 50 push ax

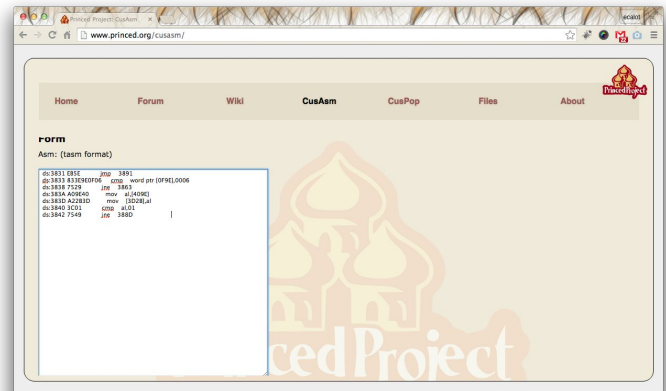
ds:0000 CD 20 7D 9D 00 E4 FF FF = 10 0
ds:0008 AD 32 0B C3 05 6B 07 1124
ds:0010 14 03 28 08 14 03 92 01
ds:0018 01 01 01 00 02 04 FF FF 800
ds:0020 FF FF FF FF FF FF FF FF

ds:1002 75C6
ds:1009 75AF
ds:0FFE FFFF
ds:0FFC 2300
ds:0FFA 3600

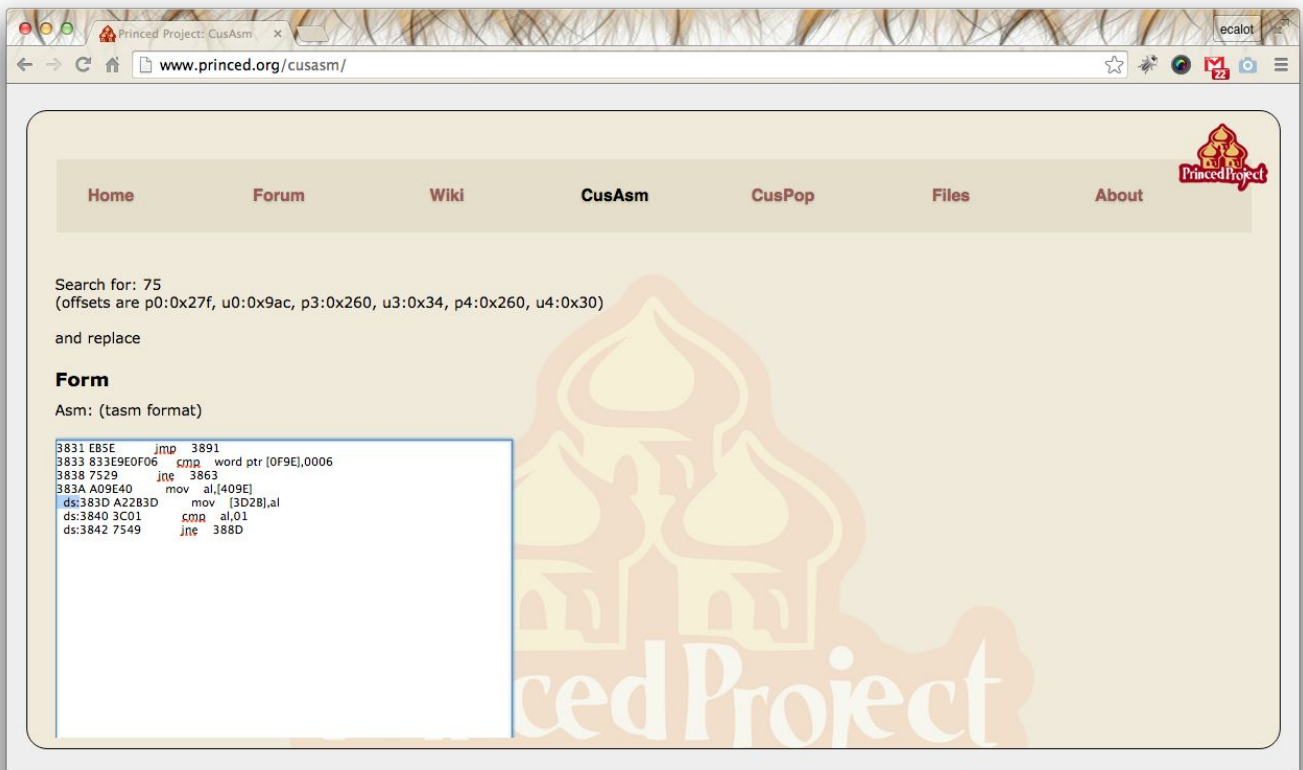
```

Copy the right lines from the file to cusasm

```
Turbo Debugger Log
PRINCE.LOG
CPU 80486
CPU code : 0869:3831 EB 5E 83 3E 9E 0F 06 75 29 A0 9E 40 A2 2B 3D 3C 01 75 49
ds:3831 EB5E jmp 3891
ds:3833 833E9E0F06 cmp word ptr [0F9E],0006
ds:3838 7529 jne 3863
ds:383A A09E40 mov al,[409E]
ds:383D A22B3D mov [3D2B],al
ds:3840 3C01 cmp al,01
ds:3842 7549 jne 388D
ds:3844 833E9C404D cmp word ptr [409C],004D
ds:3849 740F je 385A
ds:384B B81900 mov ax,0019
ds:384E 50 push ax
ds:384F 9AC5127908 call 0079:12C5
ds:3854 C7069C404D08 mov word ptr [409C],004D
ds:385A B8EABE mov ax,0EAB
```



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=""/>
```