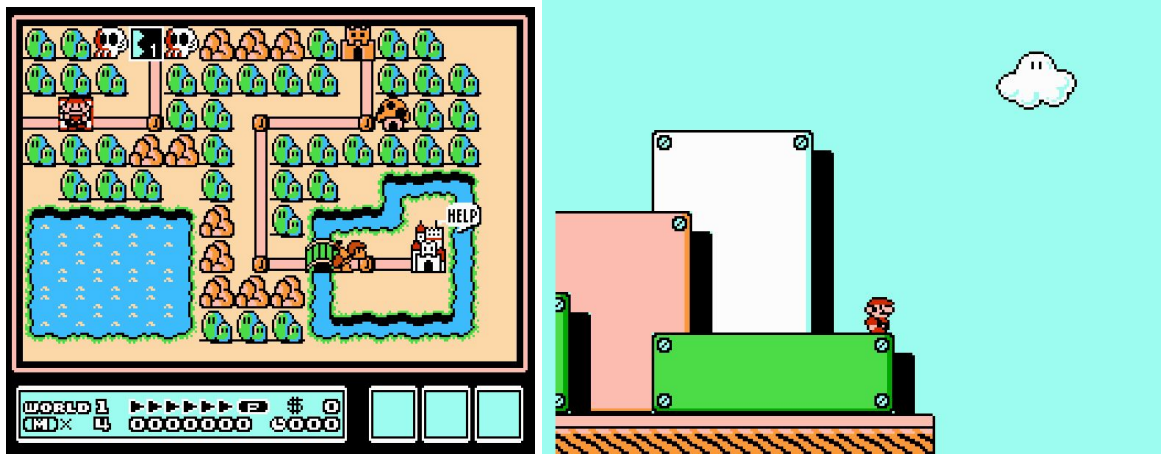


Tenemos una rom de nintendo

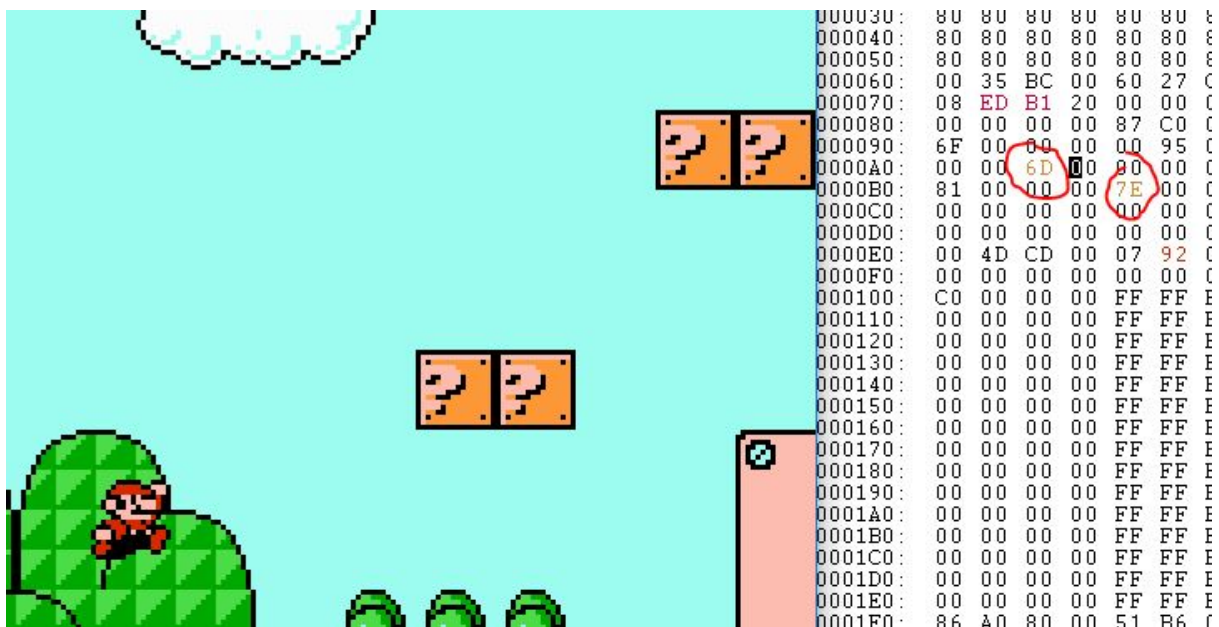
Podemos abrir esta rom con un emulador de nintendo

vemos que tenemos un único nivel imposible de llegar hasta el final



podemos utilizar un debugger en la que podemos ver la memoria en tiempo real para buscar la direcciones de memoria de parametros del juego( ej cheatEngine) El emulador que utilizo es fceux que viene con debugger integrado

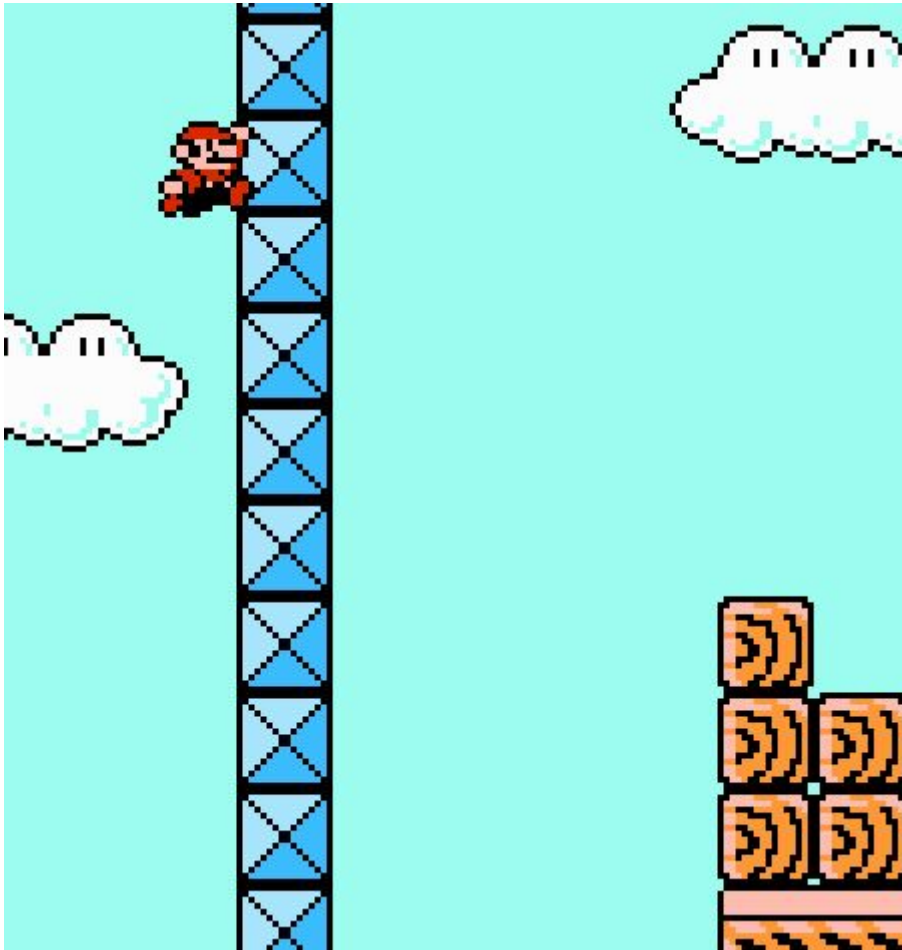
vemos que cuando mario salta cambia estos dos valores por lo tanto es la posicion y de mario



desde el propio debugger de fceux podemos modificar y congelar los valores en la dirección 0000A2 de memoria RAM



Casi llegando al final nos encontramos con una pared que no podemos pasar ni por arriba ni por abajo



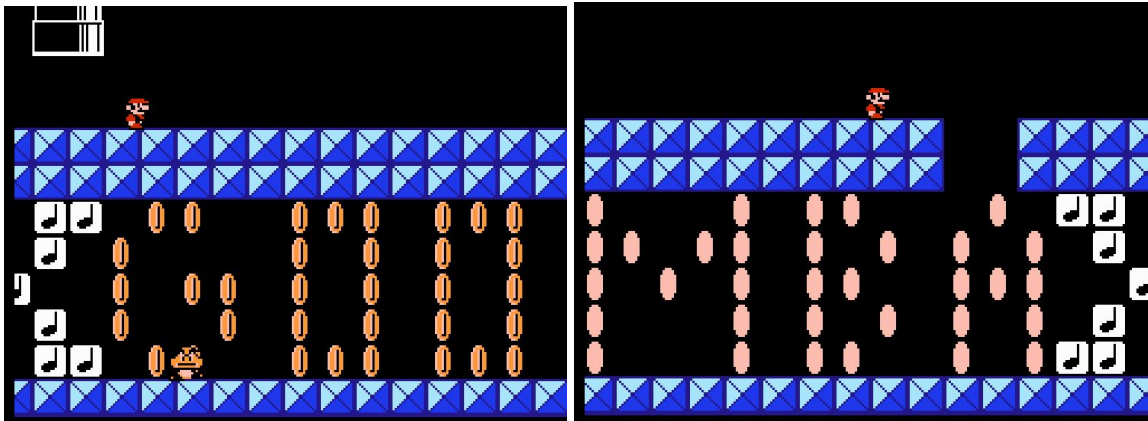
Miramos los valores de posición de mario en ram y vemos el siguiente valor en la dirección 000090 es la posición x de mario

```
000050: 80 80 80 80 80 80 80
000060: 00 3D BC 00 60 27 C5
000070: 08 ED B1 20 00 06 00
000080: 80 00 04 00 87 C0 00
000090: 23 00 00 37 68 D4 00
0000A0: 00 00 00 00 70 6F
0000B0: CF 00 00 00 21 00 00
0000C0: F8 00 08 00 00 00 00
0000D0: 00 00 00 10 00 00 00
0000E0: 00 4D CD 00 02 80 00
0000F0: 00 00 00 00 00 00 00
000100: C0 00 00 00 FF FF FF
000110: 00 00 00 00 FF FF FF
000120: 00 00 00 00 FF FF FF
```

si nos juntamos a la pared y le aumentamos el valor de la posición de x en 0x10  
atravesamos la pared



Con esto ya podemos llegar al final donde descongelamos el valor de y para poder bajar y nos encontramos una tubería y tenemos la flag escrita en monedas



flag{goomba}