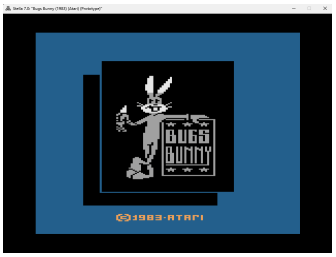
Informe de Modificación de la ROM y RAM

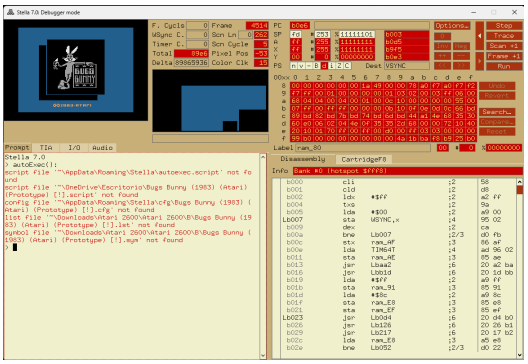


Fecha: 09/05/2025

Juego modificado: Bugs Bunny (1983) (Atari) (Prototype) [!]

1. Objetivo:

Modificar la ROM y RAM de un juego de Atari VSC (aka Atari 2600) para obtener ventajas y modificar aspectos visuales usando el depurador y emulador Stella. En este informe se modificará el juego de Bugs Bunny (1983) (Atari) (Prototype) [!].



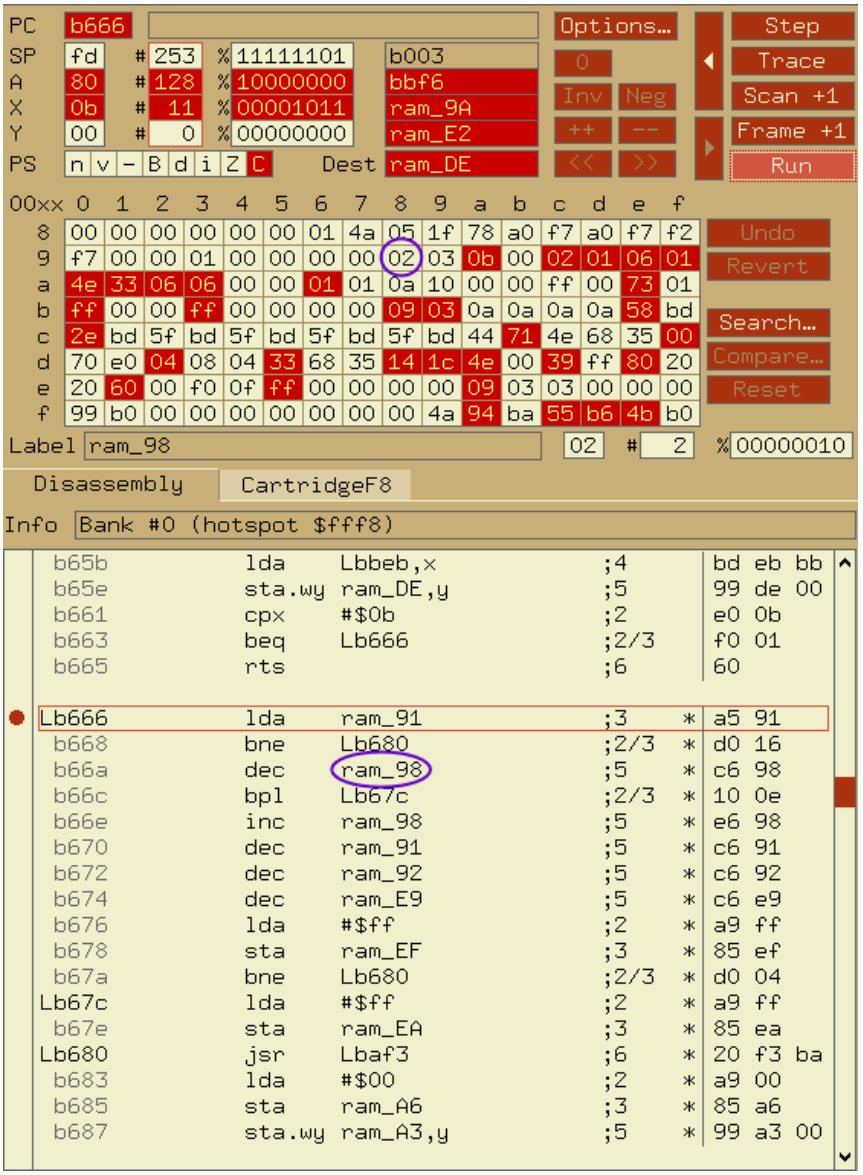
2. Variable buscada en la RAM:

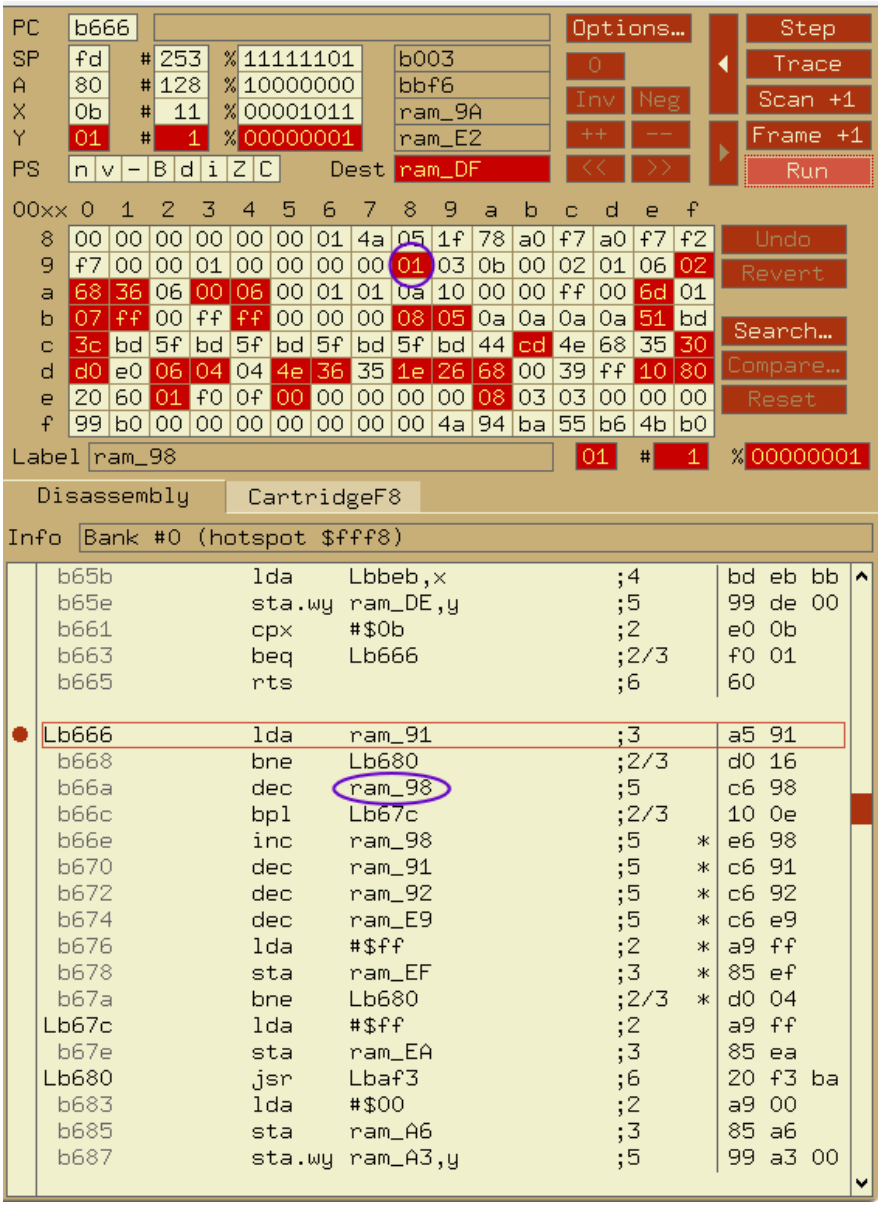
El personaje(Bugs Bunny) empieza con 3 vidas. Para obtener una ventaja en el juego y que Bugs Bunny sea inmortal necesitamos determinar donde muere en el código. Para esto vamos a usar una característica única del disassembly view. La ventana de desensamblaje (disassembly view) es una característica de Stella que muestra el código de máquina del juego de Atari en formato de código ensamblador, lo que facilita su análisis y modificación.

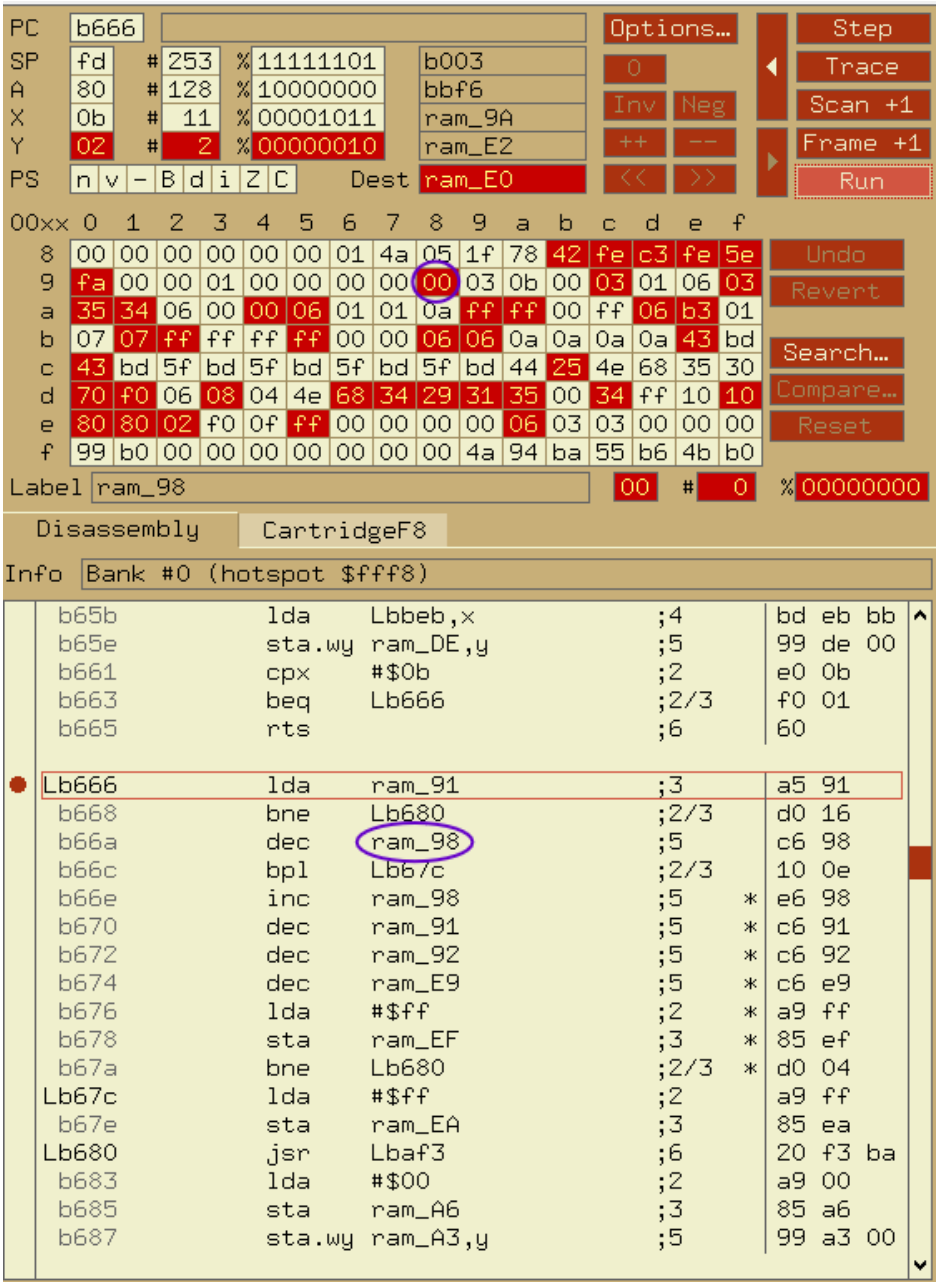
Stella tiene 2 niveles de desensamblaje. El primero es un análisis dinámico realizado por el núcleo de emulación, que realiza un seguimiento a medida que el código se ejecuta. El segundo es un análisis estático que rellena los huecos en las secciones a las que no se ha accedido en tiempo de ejecución durante el análisis dinámico. El código realizado durante el análisis estático se identifica con un asterisco. Este análisis revela propiedades que pueden ser características del juego. Estas características podrían estar ocultas, activándose solo al presionar interruptores o al suceder eventos dentro del juego, como correr, saltar, escalar e incluso morir.

En el disassembly view se usó breakpoints en direcciones de la ROM, donde estan las instrucciones, específicamente al comienzo de secciones de 10 líneas o más con asteriscos y así se pudo capturar la sección de líneas de código en donde ocurría la muerte del

personaje. Se buscaba la variable del contador de vidas, su dirección de memoria RAM es el **ram_98**. Se puede verificar que la dirección **ram_98** disminuía en 1 cuando el personaje perdía una vida. Anexo 3 capturas de pantalla de cada momento al perder una vida.




PC b666
SP fd # 253 % 11111101 b003
A 80 # 128 % 10000000 bbf6
X 0b # 11 % 00001011 ram_9A
Y 01 # 1 % 00000001 ram_E2
PS n v - B d i Z C Dest ram_DF
Options…
0
Inv Neg
++ --
<< >>
Step
Trace
Scan +1
Frame +1
Run
Undo
Revert
Search…
Compare…
Reset
00xx 0 1 2 3 4 5 6 7 8 9 a b c d e f
8 00 00 00 00 00 00 01 4a 05 1f 78 a0 f7 a0 f7 f2
9 f7 00 00 01 00 00 00 00 01 03 0b 00 02 01 06 02
a 68 36 06 00 06 00 01 01 0a 10 00 00 ff 00 6d 01
b 07 ff 00 ff ff 00 00 00 08 05 0a 0a 0a 0a 51 bd
c 3c bd 5f bd 5f bd 5f bd 5f bd 44 cd 4e 68 35 30
d d0 e0 06 04 04 4e 36 35 1e 26 68 00 39 ff 10 80
e 20 60 01 f0 0f 00 00 00 00 00 08 03 03 00 00 00
f 99 b0 00 00 00 00 00 00 00 4a 94 ba 55 b6 4b b0
Label ram_98
01 # 1 % 00000001
Disassembly
CartridgeF8
Info Bank #0 (hotspot $fff8)
b65b lda Lbbeb,x ;4 bd eb bb
b65e sta.wy ram_DE,y ;5 99 de 00
b661 cpx #$0b ;2 e0 0b
b663 beq Lb666 ;2/3 f0 01
b665 rts ;6 60
Lb666 lda ram_91 ;3 a5 91
b668 bne Lb680 ;2/3 d0 16
b66a dec ram_98 ;5 c6 98
b66c bpl Lb67c ;2/3 10 0e
b66e inc ram_98 ;5 * e6 98
b670 dec ram_91 ;5 * c6 91
b672 dec ram_92 ;5 * c6 92
b674 dec ram_E9 ;5 * c6 e9
b676 lda #$ff ;2 * a9 ff
b678 sta ram_EF ;3 * 85 ef
b67a bne Lb680 ;2/3 * d0 04
Lb67c lda #$ff ;2 a9 ff
b67e sta ram_EA ;3 85 ea
Lb680 jsr Lbaf3 ;6 20 f3 ba
b683 lda #$00 ;2 a9 00
b685 sta ram_A6 ;3 85 a6
b687 sta.wy ram_A3,y ;5 99 a3 00

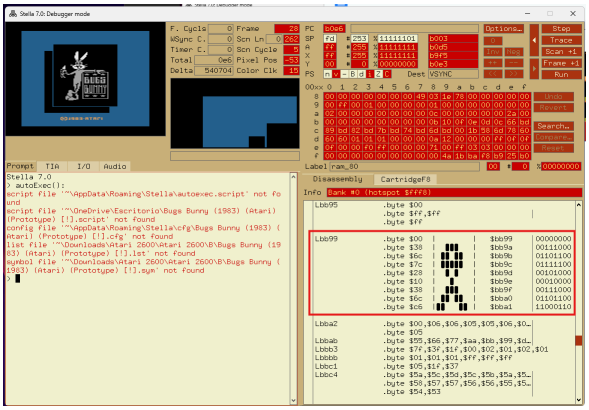


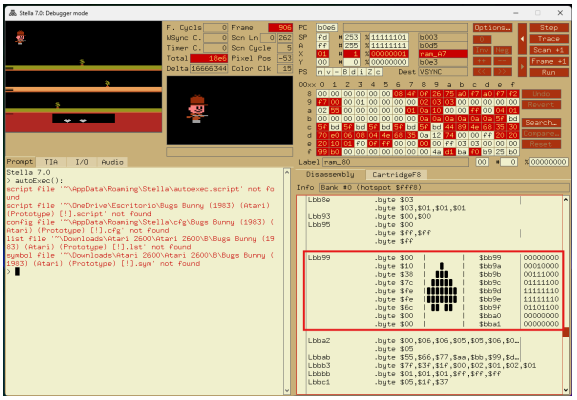
3. Modificación de la ROM:

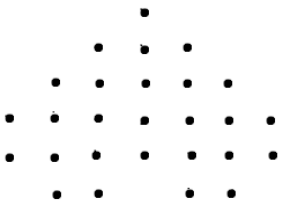
Mi objetivo es que Bugs Bunny sea inmortal, es decir, tener vidas infinitas. En la dirección de ROM **b66a** con la instrucción **dec ram_98** cuyos bytes son **c6 98** se realizó una modificación en los bytes. Se reemplazó los bytes **c6** y **98** por **ea** y **ea** respectivamente, para que no ejecute ninguna acción, en las direcciones **b66a** y **b66b**. El resultado de esta modificación hizo que el contador de vidas en **ram_98** no disminuyera al perder una vida, logrando las vidas infinitas que era nuestro objetivo. Adjunto captura de la modificación realizada.

```
Lb666           lda     ram_91          ;3      a5 91
 b668           bne     Lb680           ;2/3    d0 16
 b66a           nop                     ;2      ea
 b66b           nop                     ;2      ea
 b66c           bpl     Lb67c           ;2/3    10 0e
 b66e           inc     ram_98          ;5      e6 98
 b670           dec     ram_91          ;5      c6 91
 b672           dec     ram_92          ;5      c6 92
 b674           dec     ram_E9          ;5      c6 e9
 b676           lda     #$ff            ;2      a9 ff
 b678           sta     ram_EF          ;3      85 ef
 b67a           bne     Lb680           ;2/3    d0 04
Lb67c           lda     #$ff            ;2      a9 ff
 b67e           sta     ram_EA          ;3      85 ea
Lb680           jsr     Lbaf3           ;6      20 f3 ba
 b683           lda     #$00            ;2      a9 00
 b685           sta     ram_A6          ;3      85 a6
 b687           sta.wy  ram_A3,y        ;5      99 a3 00
 b68a           lda     #$02            ;2      a9 02
```

Por otro lado, se modificó un elemento gráfico (sprite) ubicado en la parte inferior de la ROM (accesible scrolleando hacia abajo). La modificación consistió en reemplazar la forma de las vidas, que originalmente eran la cara de Bugs Bunny, por corazones.







```
00000000
00010000
00111000
01111100
11111110
11111110
01101100
00000000
00000000
```

Dato extra: usé paint para poder dibujar el corazón invertido