

# Laboratorio Opcional De Organización Del Computador Hackeando Atari

Integrantes : Alvarez Gabriel, Garro Rosendo

Elegimos el juego 2pak en particular alien force en donde para modificar la memoria ram se hizo una modificación en ram\_AB que contiene la vida del jugador inicializada en 5. Para tener una ventaja en el juego que pueda verse en la memoria rom pensamos en rastrear el momento en el que se escribe ram\_AB para eso en la ventana de prompt se colocó un trapWrite RAM\_ab que nos arrojó los siguientes resultados

L1c9a	dec	ram_AB,x	;6	d6 ab
1c9c	bpl	L1cb2	;2/3	10 14

donde podemos ver la instrucción dec (decrementar) que esta caracterizada por el opcode d6 la modificación que se hizo es cambiar d6 por f6 creando la instrucción inc es decir la idea del hack es que cada vez que el jugador debería perder una vida gane una. Para hacer una modificación permanente buscamos hacer un reemplazo en el .bin del juego la lectura del .bin se hizo a través de bless, un editor hexadecimal luego de mucho foreo y búsqueda descubrimos que atari en algunas ocasiones mapea el offset como dirección - 1000 es por eso que L1c9a = 0c9a o bien c9a que en decimal 3226 se puede utilizar para encontrar la dirección y realizar la modificación en el lugar indicado en la imagen

00000c7b	D6	29	04	F0	E1	A9	0B	D0	02	A9	07	A2	01	60	A9	0E	D0	F9	B5	A4	29	0F	F0	F5	B4	A4	88	98	4C	C6	1D	F6	AB	00	14	A4	94	D0	10	84	96	A9	0A	95	AB
00000ca8	A9	8F	85	B6	A2	01	20	B2	1C	CA	A9	01	95	B7	A9	00	95	99	95	9F	95	AF	85	98	A9	C0	95	C6	A9	9A	A0	1E	E0	00	D0	05	85	BD	84	BE	60	85	BF	84	C0
00000cd5	60	A2	0F	B5	84	C9	54	D0	06	86	DF	A2	00	F0	08	C9	B4	D0	0B	86	DF	A2	01	A9	06	20	A5	1F	A6	DF	A9	00	95	84	CA	CA	CA	CA	10	DA	60	B5	3E	7F	

De este modo al guardar el hack se hace cada vez que se abra el juego

Finalmente se modificó la estructura del personaje para que deje de ser un canguro y sea un dinosaurio aplicando el mismo mecanismo mencionado anteriormente identificamos el offset de la primera línea que define a el canguro.

.byte \$04				\$1e00	00000100
.byte \$04				\$1e01	00000100
.byte \$07				\$1e02	00000111
.byte \$06				\$1e03	00000110
.byte \$06				\$1e04	00000110
.byte \$06				\$1e05	00000110
.byte \$0e				\$1e06	00001110
.byte \$1e				\$1e07	00011110
.byte \$3f				\$1e08	00111111
.byte \$3d				\$1e09	00111101
.byte \$7e				\$1e0a	01111110
.byte \$7e				\$3d = #61 = %00111101	
.byte \$6c				\$1e0c	01101100
.byte \$24				\$1e0d	00100100
.byte \$a8				\$1e0e	10101000
.byte \$ee				\$1e0f	11101110
.byte \$00				\$1e10	00000000
.byte \$00				\$1e11	00000000
.byte \$00				\$1e12	00000000
.byte \$00				\$1e13	00000000
.byte \$00				\$1e14	00000000
.byte \$00				\$1e15	00000000

Como se puede ver en la imagen la primera línea que define al canguro es 1e00 como mencionamos anteriormente deberíamos buscar el offset 0e00 en decimal 3584 la búsqueda se realizó en el .bin en hexadecimal como esta detallado anteriormente donde vemos que la línea mencionada contiene 04 lo que es coherente con la imagen que estamos viendo y esa la modificamos por 07 y así en todas las líneas que requieren modificación viendo que el dinosaurio esta definido 3 veces en 3 posiciones distintas las definimos todas.

Dejo a continuación todas las definiciones del dinosaurio realizadas

.byte \$00			
.byte \$07		\$1e00	00000111
.byte \$05		\$1e01	00000101
.byte \$07		\$1e02	00000111
.byte \$06		\$1e03	00000110
.byte \$06		\$1e04	00000110
.byte \$06		\$1e05	00000110
.byte \$0e		\$1e06	00001110
.byte \$1e		\$1e07	00011110
.byte \$3f		\$1e08	00111111
.byte \$3d		\$1e09	00111101
.byte \$7e		\$1e0a	01111110
.byte \$7e		\$1e0b	01111110
.byte \$6c		\$1e0c	01101100
.byte \$44		\$1e0d	01000100
.byte \$48		\$1e0e	01001000
.byte \$6e		\$1e0f	01101110
.byte \$00		\$1e10	00000000
.byte \$00		\$1e11	00000000
.byte \$00		\$1e1a	00000000
.byte \$00		\$1e1b	00000000
.byte \$07		\$1e1c	00000111
.byte \$05		\$1e1d	00000101
.byte \$07		\$1e1e	00000111
.byte \$06		\$1e1f	00000110
.byte \$06		\$1e20	00000110
.byte \$06		\$1e21	00000110
.byte \$0e		\$1e22	00001110
.byte \$1e		\$1e23	00011110
.byte \$3f		\$1e24	00111111
.byte \$3d		\$1e25	00111101
.byte \$7e		\$1e26	01111110
.byte \$7e		\$1e27	01111110
.byte \$28		\$1e28	00101000
.byte \$28		\$1e29	00101000
.byte \$ee		\$1e2a	11101110
.byte \$00		\$1e2b	00000000
.byte \$00		\$1e2c	00000000

.byte \$00		\$1e19	00000000
.byte \$00		\$1e1a	00000000
.byte \$00		\$1e1b	00000000
.byte \$07		\$1e1c	00000111
.byte \$05		\$1e1d	00000101
.byte \$07		\$1e1e	00000111
.byte \$06		\$1e1f	00000110
.byte \$06		\$1e20	00000110
.byte \$06		\$1e21	00000110
.byte \$0e		\$1e22	00001110
.byte \$1e		\$1e23	00011110
.byte \$3f		\$1e24	00111111
.byte \$3d		\$1e25	00111101
.byte \$7e		\$1e26	01111110
.byte \$7e		\$1e27	01111110
.byte \$28		\$1e28	00101000
.byte \$28		\$1e29	00101000
.byte \$ee		\$1e2a	11101110
.byte \$00		\$1e2b	00000000
.byte \$00		\$1e2c	00000000

.byte \$04				\$1e00		00000100
.byte \$04				\$1e01		00000100
.byte \$07				\$1e02		00000111
.byte \$06				\$1e03		00000110
.byte \$06				\$1e04		00000110
.byte \$06				\$1e05		00000110
.byte \$0e				\$1e06		00001110
.byte \$1e				\$1e07		00011110
.byte \$3f				\$1e08		00111111
.byte \$3d				\$1e09		00111101
.byte \$7e				\$1e0a		01111110
.byte \$7e				\$3d = #61 = %00111110		
.byte \$6c				\$1e0c		01101100
.byte \$24				\$1e0d		00100100
.byte \$a8				\$1e0e		10101000
.byte \$ee				\$1e0f		11101110
.byte \$00				\$1e10		00000000
.byte \$00				\$1e11		00000000
.byte \$00				\$1e12		00000000
.byte \$00				\$1e13		00000000
.byte \$00				\$1e14		00000000
.byte \$00				\$1e15		00000000

.byte \$00				\$1e32		00000000
.byte \$00				\$1e33		00000000
.byte \$00				\$1e34		00000000
.byte \$00				\$1e35		00000000

.byte \$00

.byte \$04				\$1e37		00000100
.byte \$07				\$1e38		00000111
.byte \$06				\$1e39		00000110
.byte \$06				\$1e3a		00000110
.byte \$06				\$1e3b		00000110
.byte \$0e				\$1e3c		00001110
.byte \$1e				\$1e3d		00011110
.byte \$3e				\$1e3e		00111110
.byte \$3e				\$1e3f		00111110
.byte \$7e				\$1e40		01111110
.byte \$7e				\$1e41		01111110
.byte \$ac				\$1e42		10101100
.byte \$ac				\$1e43		10101100
.byte \$ee				\$1e44		11101110
.byte \$00				\$1e45		00000000
.byte \$00				\$1e46		00000000