Maquina del mal

1. pip install pyevmasm
   Ejecutar

```
from pyevmasm import disassemble_hex
bytecode =
'0x61951d636063eb0c04613b83346063613f7260b4080203602c611af3026107a4526207d
0b961ab52016107c75262026a8561952d18620881ba526107c7516107a4510214604857ff
00'
print(disassemble_hex(bytecode))
```

1. consola

```
PUSH2 0x951d
PUSH4 0x6063eb0c
DIV
PUSH2 0x3b83
CALLVALUE
PUSH1 0x63
PUSH2 0x3f72
PUSH1 0xb4
ADDMOD
MUL
SUB
PUSH1 0x2c
PUSH2 0x1af3
MUL
PUSH2 0x7a4
MSTORE
PUSH3 0x7d0b9
PUSH2 0xab52
ADD
PUSH2 0x7c7
MSTORE
PUSH3 0x26a85
PUSH2 0x952d
XOR
PUSH3 0x881ba
MSTORE
```

```
PUSH2 0x7c7
MLOAD
PUSH2 0x7a4
MLOAD
MUL
EQ
PUSH1 0x48
JUMPI
SELFDESTRUCT
STOP
```

1. Analisis

```
PUSH2 0x951d # = 38173 [0x951d]
PUSH4 0x6063eb0c # = 1679497972 [0x951d, 0x6063eb0c]
DIV # 1617597196/38173 = 42364 = 0xa57c [0xa57c]
PUSH2 0x3b83  # = 15235 [0xa57c, 0x3b83]
CALLVALUE # Valor a encontrar [0xa57c, 0x3b83, CALLVALUE]
PUSH1 0x63 # = 99 [0xa57c, 0x3b83, CALLVALUE, 0x63]
PUSH2 0x3f72 # = 16242 [0xa57c, 0x3b83, CALLVALUE, 0x63, 0x3f72]
PUSH1 0xb4 # = 180 [0xa57c, 0x3b83, CALLVALUE, 0x63, 0x3f72, 0xb4]
ADDMOD # (0xb4 + 0x3f72) mod 0x63 = (180 + 16242) mod 99 = 16422 mod 99 = 87 = 0x57
[0xa57c, 0x3b83, CALLVALUE, 0x57]
MUL # 99 * 87 = 8613 [0xa57c, 0x3b83, CALLVALUE*0x57]
SUB # x - 8613 [0xa57c, CALLVALUE*0x57 - 0x3b83]
PUSH1 0x2c # = 44 [0xa57c, CALLVALUE*0x57 - 0x3b83, 0x2c]
PUSH2 0x1af3 # = 6899 [0xa57c, CALLVALUE*0x57 - 0x3b83, 0x2c, 0x1af3]
MUL # 44 * 6899 = 0x4a1c4 = 303556 [0xa57c, CALLVALUE*0x57 - 0x3b83, 0x4a1c4]
PUSH2 0x7a4 = 1956 [0xa57c, CALLVALUE*0x57 - 0x3b83, 0x4a1c4, 0x7a4]
MSTORE # memory[0x7a4] = 0x4a1c4 = 303556 [0xa57c, CALLVALUE*0x57 - 0x3b83]
PUSH3 0x7d0b9 # = 512185 [0xa57c, CALLVALUE*0x57 - 0x3b83, 0x7d0b9]
PUSH2 0xab52 # = 43858 [0xa57c, CALLVALUE*0x57 - 0x3b83, 0x7d0b9, 0xab52]
ADD # 512185 + 43858 = 556043 [0xa57c, CALLVALUE*0x57 - 0x3b83, 0x87c0b]
PUSH2 0x7c7 [0xa57c, CALLVALUE*0x57 - 0x3b83, 0x87c0b, 0x7c7]
MSTORE # mem[0x7c7] = 556043 [0xa57c, CALLVALUE*0x57 - 0x3b83]
PUSH3 0x26a85 # = 158341 [0xa57c, CALLVALUE*0x57 - 0x3b83, 0x26a85]
PUSH2 0x952d # = 38189 [0xa57c, CALLVALUE*0x57 - 0x3b83, 0x26a85, 0x952d]
XOR # = 120712 [0xa57c, CALLVALUE*0x57 - 0x3b83, 0x2ffa8]
```

```
PUSH3 0x881ba [0xa57c, CALLVALUE*0x57 - 0x3b83, 0x2ffa8, 0x881ba]
MSTORE # = 557370 # mem[0x881ba] = 120712 [0xa57c, CALLVALUE*0x57 - 0x3b83]
PUSH2 0x7c7 [0xa57c, CALLVALUE*0x57 - 0x3b83, 0x7a4]
MLOAD # = 556043 [0xa57c, CALLVALUE*0x57 - 0x3b83, 0x87c0b]
PUSH2 0x7a4 [0xa57c, CALLVALUE*0x57 - 0x3b83, 0x87c0b, 0x7a4]
MLOAD # = 303556 [0xa57c, CALLVALUE*0x57 - 0x3b83, 0x87c0b, 0x4a1c4]
MUL # = 556043 * 303556 [0xa57c, CALLVALUE*0x57 - 0x3b83, 0x274cade36c]
EQ [0xa57c, CALLVALUE*0x57 - 0x3b83 == 0x274cade36c]
PUSH1 0x48 [0xa57c, CALLVALUE*0x57 - 0x3b83 == 0x274cade36c, 0x42]
JUMPI
SELFDESTRUCT
STOP
```

1. Operaciones

CALLVALUE*0x57 - 0x3b83 == 0x274cade36c
CALLVALUE = (0x274cade36c + 0x3b83)/0x57
CALLVALUE = 0x73a3d729 = 1940117289
0x73a3d729 = 1940117289

Respuesta Flag UVT{0x73a3d729}