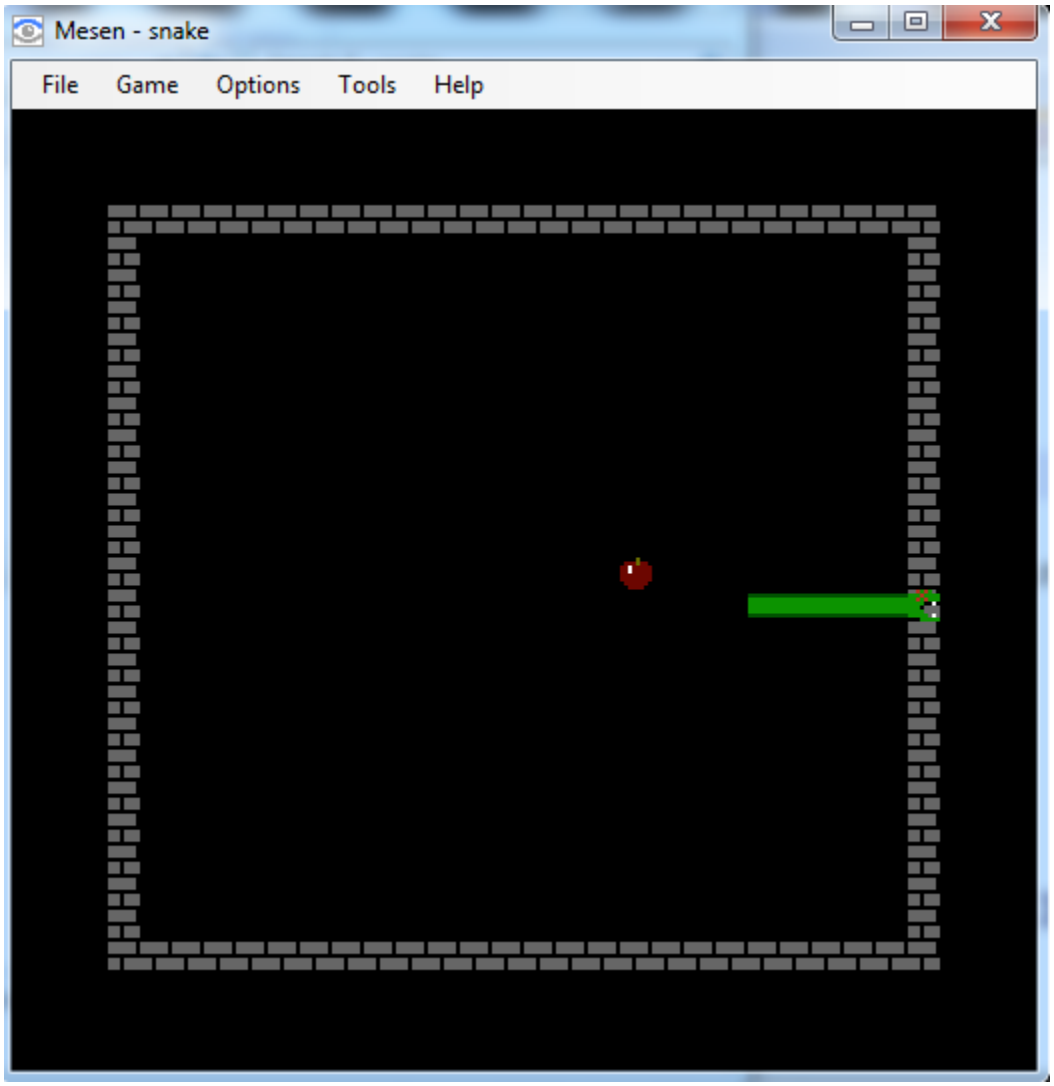
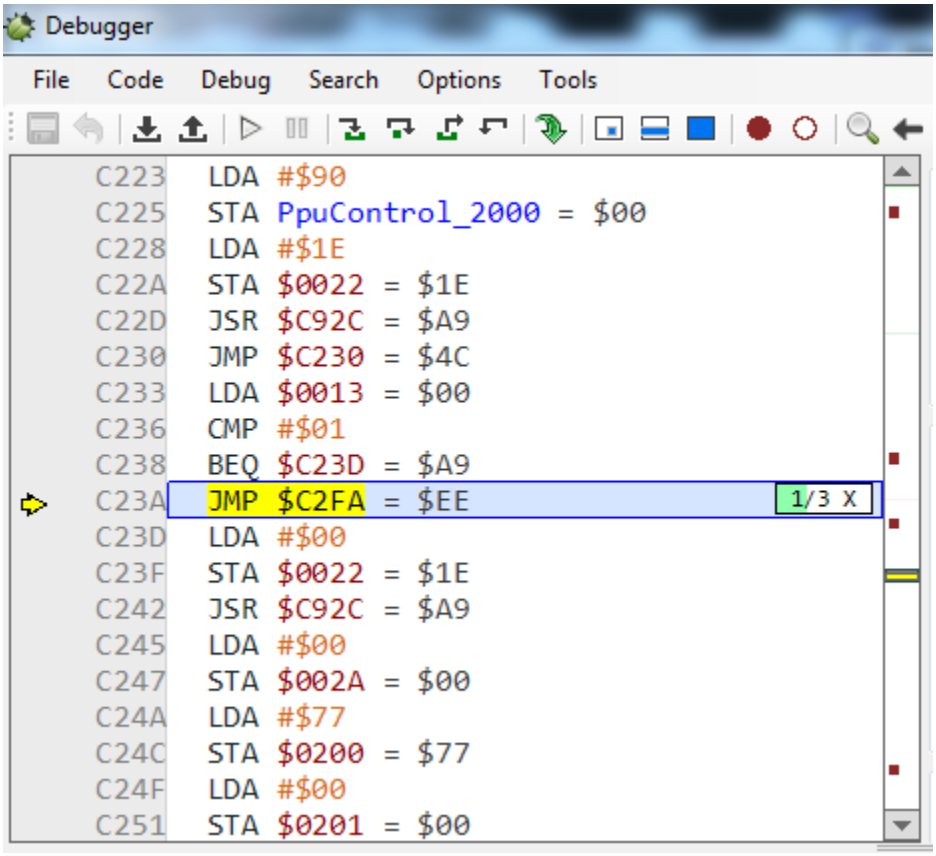
Snake

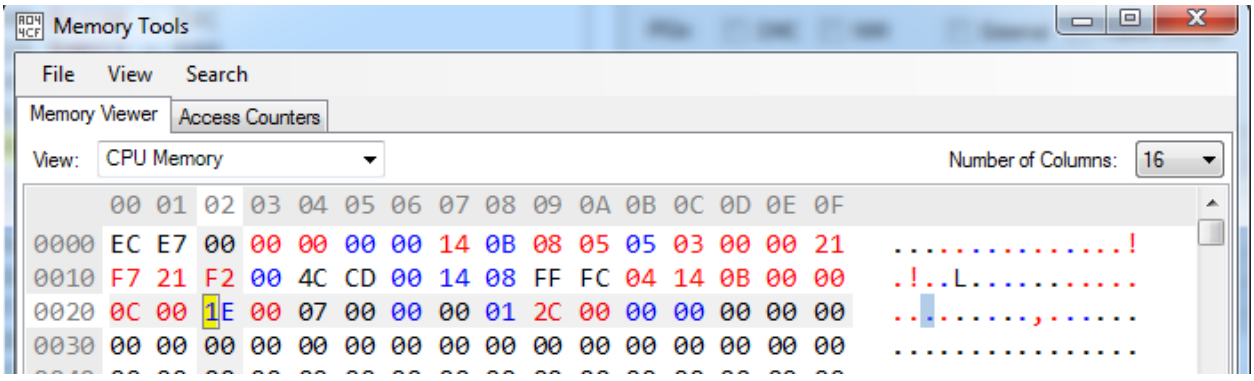
Challenge này là một ROM NES, sử dụng mesen để chạy ROM



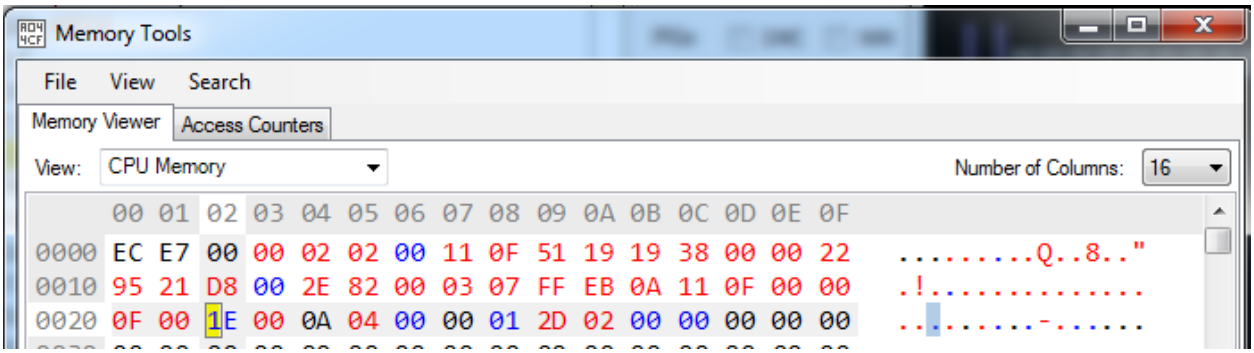
Màn hình debug của mesen



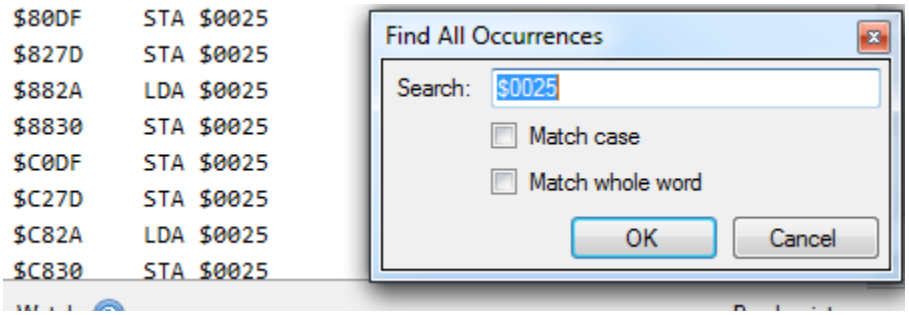
Sau một hồi kiểm tra memory một số địa chỉ thường được load và compare thì ta có 1 phân vùng memory có các giá trị như sau:



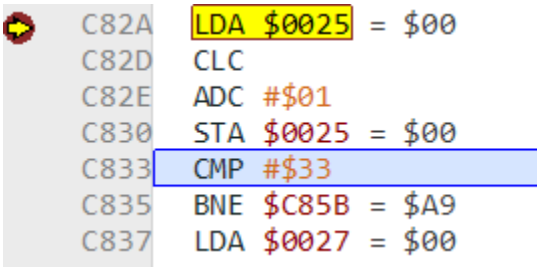
Tiếp tục chơi game và quan sát sau khi ăn 4 quả táo thì thấy địa chỉ 0x25 trở thành số 4 từ đó ta có thể đoán đây là địa chỉ chứa giá trị số táo đã ăn được



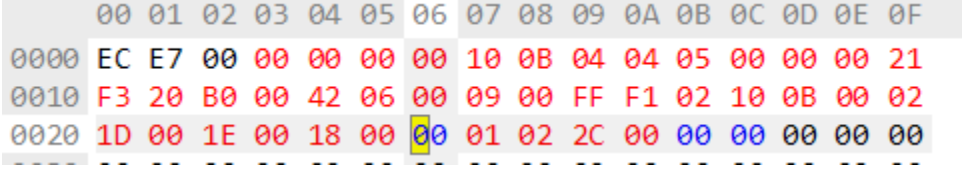
Ta tìm xem $0025 có trong các dòng lệnh nào và test xem mỗi khi snake cắn 1 quả táo game sẽ break ở đâu



Và sau một vài lần thử thì ta có:



Nếu cắn đủ 0x33 quả táo thì sẽ load $0027, do lệnh CMP trong này là == nên ta thử sửa giá trị trong $0025 thành 0x32 và cắn thêm 1 quả táo



Ta thấy $0027 tăng 1 vào $0028 tăng 2

Check đoạn code sau LDA $0027 ta thấy

```
C833   CMP #$33
C835   BNE $C85B = $A9
C837   LDA $0027 = $01
C83A   CLC
C83B   ADC #$01
C83D   STA $0027 = $01
C840   CMP #$04
```

Lúc này ta chỉnh $0025 thành 0x32 và $0027 thành 0x3 và cắn thêm 1 quả táo

```
     00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0000 EC E7 00 00 03 03 00 00 0A 1B 05 0A 16 01 01 21
0010 A4 21 88 00 1A E5 00 00 0A FF E8 0D 00 0A 00 00
0020 15 00 1E 00 10 32 00 03 02 2D 03 00 00 00 00 00
```

Ta được Flag