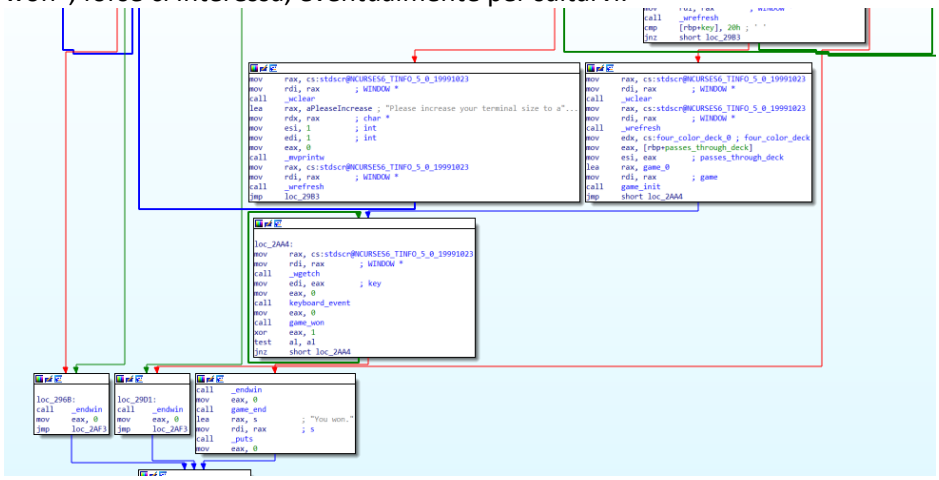
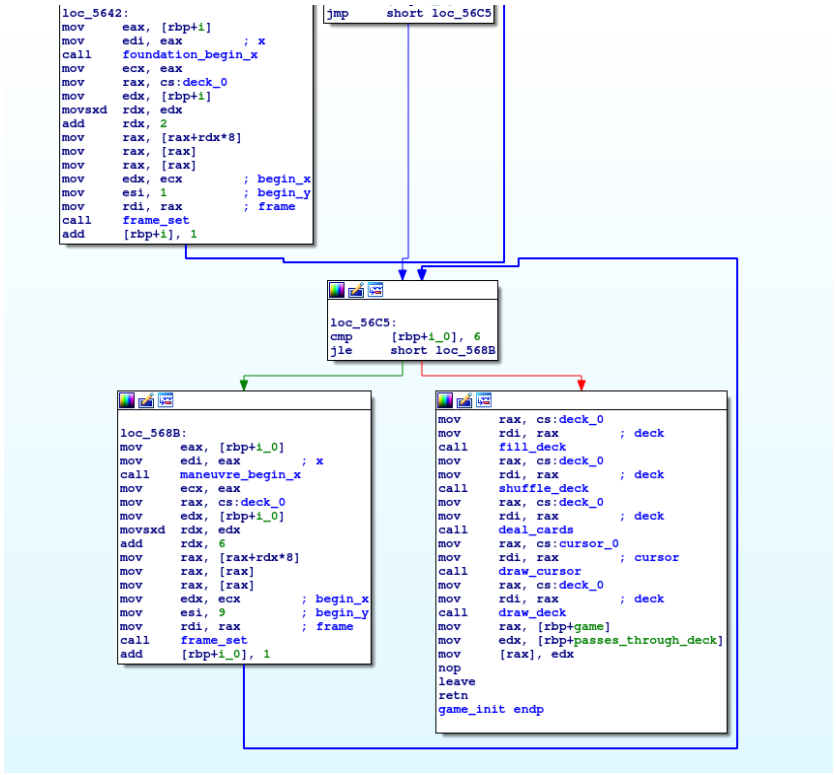
Soluzione

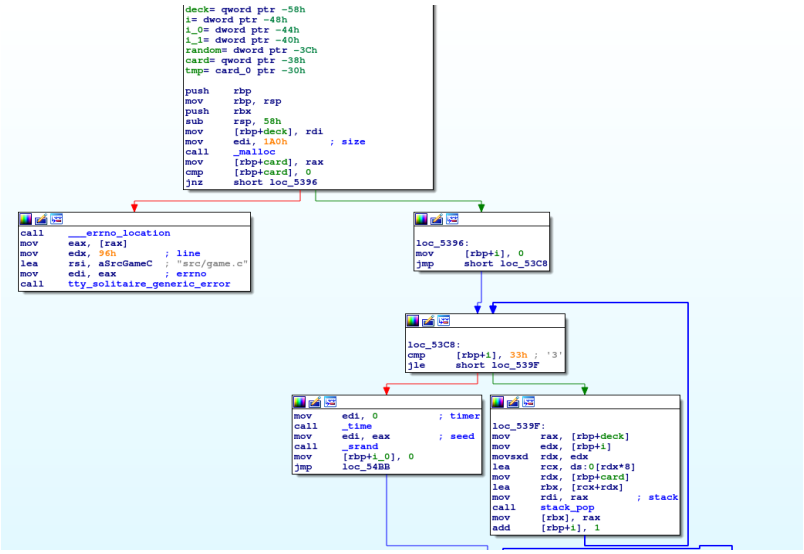
Aprendo il binario in IDA, vediamo un bel numero di funzioni. Ognuna di queste serve a inizializzare le carte, spostarle, mescolarle, riempirle, etc.
Dal momento che vogliamo che la mano iniziale sia sempre la stessa, potremmo cercare una chiamata a una funzione casuale che inizializza il mazzo. Aprendo il *main* con IDA, possiamo notare la stringa “you won”; forse ci interessa, eventualmente per saltarvi.



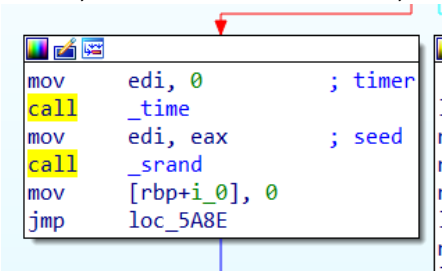
Nello stesso blocco, esiste un *keyboard_event* invocato, che associa tutte le mosse del gioco e fanno capire di chiamare altre funzioni; nello specifico, tutte quelle del gioco (che non dettagliamo). A questo punto, possiamo andare ad ispezionare, idealmente, la funzione che avvia le partite, quindi *game_init* tra la lista delle funzioni.



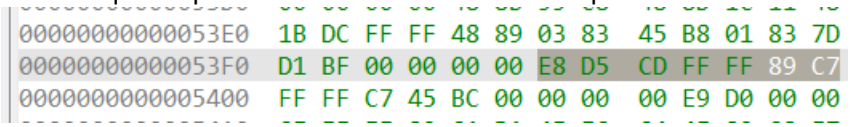
Possiamo notare tra tutte le chiamate spostamenti di carte, cursori, mazzi e varie cose. In particolare, salta all’occhio la funzione *shuffle_deck*.



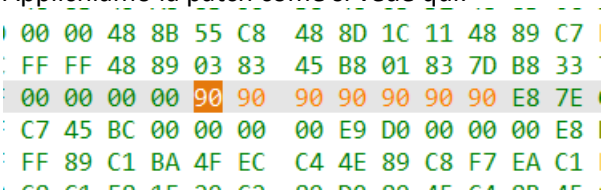
Finalmente abbiamo trovato una chiamata *_srand*, il che significa che chiama la funzione casuale per generare l'ordine delle carte nel mazzo. Prima di esso, vediamo una chiamata *_time* e il risultato viene messo in *edi* prima della chiamata *_srand*. Ciò significa fondamentalmente che utilizza la funzione *_time* per generare il seme da alimentare nel random. Quindi, se rimuoviamo la chiamata a _time e il *mov edi,eax*, in *edi* avremo sempre 0 (nota l'istruzione subito prima di chiamare *_time*). Basta scrivere NOP su queste due istruzioni (*call _time* e *mov edi, eax*), e il gioco è fatto.
Quindi, tra IDA View ed Hex View, avremo:



Patch di questo pezzo evidenziato in IDA che comprende entrambe le istruzioni:



Applichiamo la patch come si vede qui:



(quindi, vuol dire cliccare dove ci sono le due istruzioni call e mov, andare su “Hex View” e scrivere 90 su tutti i blocchi di byte word che comprendono le due istruzioni → solo quelli).
Poi, si applica il risultato con

1. Edit > Patch program > Apply patches to input file…
2. Confermare l'operazione

Teoricamente, si dovrebbe giocare e capire se si vince. In pratica, non esiste una flag di riferimento, quindi ci accontenti di quanto fatto finora.