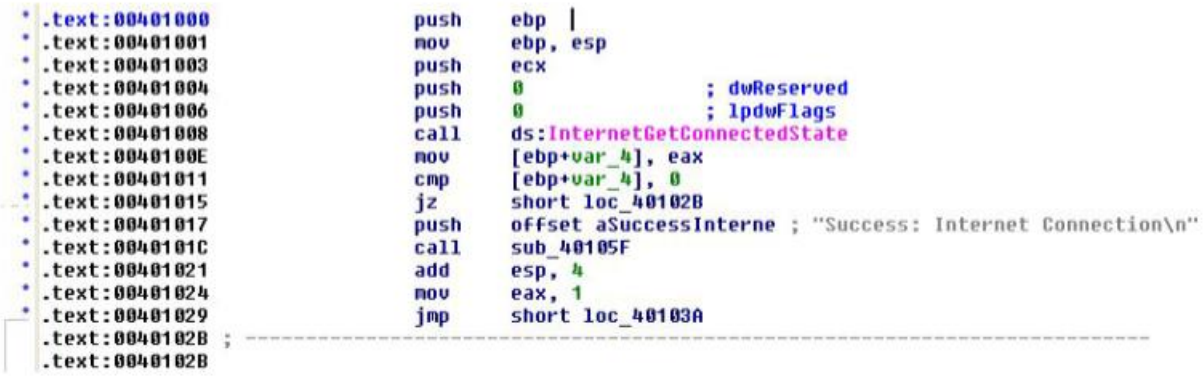
ANALISI CODICE ASSEMBLY

Consegna:

1. Identificare i costrutti noti (es. while, for, if, switch, ecc.)
2. Ipotizzare la funzionalità – esecuzione ad alto livello
3. Bonus: studiare e spiegare ogni singola riga di codice



1. IDENTIFICARE I COSTRUTTI NOTI

Con certezza , possiamo dire che cmp e jz posso essere tradotti in linguaggio C come un costrutto IF, mentre il jmp alla fine non sappiamo a cosa si riferisca perché salta ad una locazione di memoria che non conosciamo.

2. IPOTIZZARE LA FUNZIONALITA’

Il codice permette di controllare se la macchina è connessa ad Internet.

3. SPIEGARE OGNI RIGA DEL CODICE

Le prime 2 righe servono per creare lo stack, i successivi 3 push ed il call servono a passare i parametri alla funzione, che in questo caso è InternetGetConnectedState, funzione che permette di controllare se la macchina è connessa ad Internet;

con la riga sotto si sposta il contenuto del registro EAX all’interno di EBP, si compara poi il registro EBP con lo 0, se il risultato è uguale a zero, salta alla locazione di memoria 40102B;

il push mette in cima allo stack la stringa che verrà immagino stampata dal call sotto che chiama una funzione alla locazione 40105F;

si aggiunge l’intero 4 al registro ESP e si sposta 1 all’interno di EAX, mentre jmp salta alla locazione di memoria 40103A