ANALISI DI CODICE IN ASSEMBLY

```
.text:00401000                  push    ebp
.text:00401001                  mov     ebp, esp
.text:00401003                  push    ecx
.text:00401004                  push    0               ; dwReserved
.text:00401006                  push    0               ; lpdwFlags
.text:00401008                  call    ds:InternetGetConnectedState
.text:0040100E                  mov     [ebp+var_4], eax
.text:00401011                  cmp     [ebp+var_4], 0
.text:00401015                  jz      short loc_40102B
.text:00401017                  push    offset aSuccessInterne ; "Success: Internet Connection\n"
.text:0040101C                  call    sub_40105F
.text:00401021                  add     esp, 4
.text:00401024                  mov     eax, 1
.text:00401029                  jmp     short loc_40103A
.text:0040102B ; ---------------------------------------------------------------------------
.text:0040102B
```

Identificazione dei costrutti

Possiamo notare che in questa sezione di codice sia presente una comparazione tra la variabile [ebp+var_4] e 0.
In quella successiva notiamo una condizionale, ovvero, se il risultato della condizionale e' uguale a 0 passa direttamente alla parte di codice indicata dalla riga.

In questo caso sembra chiaro che il codice si riferisca ad un costrutto if

In questo ci riferiaimo ad una istruzione nota che ci indica di passare direttamente alla riga di codice indicata nel comando

IPOTESI DI FUNZIONAMENTO

Da questa parte di codice indicata dalla traccia possiamo capire che si stia effettuando una verifica della connessione a internet.Nel caso in cui ci sia una connessione ci sara un print di <success: Internet connection.>

```
.text:00401000                 push    ebp
.text:00401001                 mov     ebp, esp
.text:00401003                 push    ecx
.text:00401004                 push    0                       ; dwReserved
.text:00401006                 push    0                       ; lpdwFlags
.text:00401008                 call    ds:InternetGetConnectedState
.text:0040100E                 mov     [ebp+var_4], eax
.text:00401011                 cmp     [ebp+var_4], 0
.text:00401015                 jz      short loc_40102B
.text:00401017                 push    offset aSuccessInterne ; "Success: Internet Connection\n"
.text:0040101C                 call    sub_40105F
.text:00401021                 add     esp, 4
.text:00401024                 mov     eax, 1
.text:00401029                 jmp     short loc_40103A
.text:0040102B ; ---------------------------------------------------------------------------
.text:0040102B
```

inserisce il valore di ebp nella stack

copia i valori di esp in ebp

inserisce il valore di ecx nello stack

stiamo dando il valore 0 ai parametri della funzione

stiamo richiamando la funzione

copiamo il valore di eax nella variabile var_4

qui indichiamo la condizione

qui ci dice che la connessione ha successo

richiama una subroutine

chiudiamo la funzione

assegnamo il valore 1 al registro

andiamo alla riga di codice indicata

questo sembrerebbe essere un commento o una nota di chi ha scritto il codice