Costrutti C – Assembly x86

1)Identificare i costrutti noti :

La prima richiesta della traccia di oggi era quella di identificare nel nostro codice assembly eventuali costrutti. Nel nostro caso si può notare:

```
cmp    [ebp+var_4], 0
jz    short loc_401102B
push    offeset aSeccessInterne ;
call    sub_40105F
add    esp,    4
mov    eax, 1
jmp    short loc_40103A
```

Come si può notare le prime due righe di codice sembrano essere un **if else .** Si nota dal fatto che il **cmp** compara **[ebp+var_4] con zero,** in caso il risultato sia diverso da 0 le istruzioni continueranno in modo continuo,questo è la struttura di un **if**. In caso invece il risultato sia 0 l' istruzione **jz** fa saltare il programma a **short loc_401102B** che può essere interpretato come l' operando **else**.

2) Ipotizzare la funzionalità – esecuzione ad alto livello :

Dalle poche righe di codice a nostra disposizione si può notare dalle istruzioni **call ds:InternetGetConnectedState** e **push offeset aSeccessInterne** che il nostro pezzo di codice verifichi che una macchina sia connessa ad internet.

3) Bonus – studiare e spiegare ogni singola riga del codice :

```
push    ebp
```
Si mette in memoria il registro ebp.

```
mov    ebp, esp
```
con questa operazione di crea poi lo stack.

```
push    ecx
```
si inserisce nello stack ecx.

```
push    0          ; dwReserved
```
si passano i parametri per la funzione, sempre nello stack.

```
push    0          ;lpdwFlags
```
si passano i parametri per la funzione, sempre nello stack.

```
call    ds:InternetGetConnectedState
```
una volta inseriti i parametri si richiama la funzione.

```
mov    [ebp+var4], eax
```
sposta eax nel locazione di memoria puntata da **[ebp+var4].**

```
cmp    [ebp+var_4], 0
```
compara il valore di [ebp+var4] con 0.

jz short loc_401102B
nel caso il confronto sopra produca come risultato 0 il comando eseguirà il salto.

push offeset aSeccessInterne ;”Success: Internet Connection\n”
inserisce in memoria la stringa offeset aSeccessInterne.

call sub_40105F
richiama sub_40105F che potrebbe essere una procedura o simile.

add esp, 4
somma al registro esp il valore decimale 4.

mov eax, 1
sposta il valore decimale 1 nel registro eax.

jmp short loc_40103A
effettua un jump non condizionale verso short loc_40103A.

```
push    ebp
mov    ebp, esp
push    ecx
push    0           ; dwReserved
push    0           ;lpdwFlags
call    ds:InternetGetConnectedState
mov    [ebp+var4], eax
cmp    [ebp+var_4], 0
jz    short loc_401102B
push    offeset aSeccessInterne ;”Success: Internet Connection\n”
call    sub_40105F
add    esp,    4
mov    eax, 1
jmp    short loc_40103A
```