Nell'esercizio di oggi ci viene chiesto di esaminare il codice assembly di seguito ed identificare i costrutti C equivalenti. Inoltre provare a ipotizzare la funzionalità del codice.

```
push
.text:00401000
                                         ebp
.text:00401001
                                 mov
                                         ebp,
.text:00401003
                                 push
                                         ecx
.text:00401004
                                 push
                                         0
                                                            dwReserved
.text:00401006
                                                          ; lpdwFlags
                                 push
.text:00401008
                                 call
                                         ds:InternetGetConnectedSt
.text:0040100E
                                         [ebp+var_4], eax
                                 mov
.text:00401011
                                         [ebp+var 4],
                                 CMD
.text:00401015
                                         short loc 40102B
.text:00401017
                                 push
                                         offset aSuccessInterne ; "Success: Internet Connection\n"
                                         sub_40105F
.text:0040101C
                                 call
.text:00401021
                                 add
                                         esp, 4
.text:00401024
.text:00401029
                                         short loc_40103A
.text:0040102B
.text:0040102B
```

Nel codice si possono identificare tre costrutti. Un ciclo if, la creazione dello stack nella memoria e il passaggio dei parametri alla funzione. Nella figura sotto viene evidenziato il ciclo if:

```
.text:00401000
                                 push
                                          ebp
.text:00401001
                                          ebp, esp
                                 mov
.text:00401003
                                 push
                                          ecx
.text:00401004
                                 push
                                                           ; dwReserved
.text:00401006
                                                           ; lpdwFlags
                                 push
.text:00401008
                                          ds:InternetGetConnectedState
                                 call
.text:0040100E
                                          [ebo+var 4].
                                 mov
                                          [ebp+var 4], 0
.text:00401011
                                спр
.text:00401015
                                          short loc 40102B
                                 iz
.text:00401017
                                          offset asuccessinterne ; "Success: Internet Connection\n"
                                 DUSN
.text:0040101C
                                          sub 40105F
                                 call
.text:00401021
                                 add
                                         esp, 4
eax, 1
.text:00401024
                                          eax,
                                 mov
.text:00401029
                                         short loc 40103A
                                 imp
.text:0040102B
.text:0040102B
```

L'istruzione "jz" esegue un salto alla locazione specificata quando lo zero flag è uguale a 1, ovvero quando il risultato della sottrazione è uguale a 0. Quindi l'istruzione "cmp" serve a capire se la variabile 4 è uguale a 0.

La funzione di questo codice sembra essere quella di capire se c'è una connessione disponibile con la quale raggiungere internet. Se la condizione del ciclo non è soddisfatta verrà stampato a schermo "Success: Internet Connection" altrimenti verrà effettuato il salto a una locazione 40102B riportata più in basso.

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

Nell'immagine sopra viene evidenziato la parte di codice in cui viene creato lo stack della funzione, mentre in quella sotto il passaggio dei parametri alla funzione tramite il comando "push".

```
* .text:00401000
                                   push
  .text:00401001
                                   mov
                                           ebp,
  .text:00401003
                                  push
                                           ecx
                                                            ; dwReserved
  .text:00401004
                                   push
                                           8
 .text:00401006
                                  push
                                                            ; lpdwFlags
                                           as:InternetGetConnectedState
  .text:00401008
                                   call
                                           [ebp+var_4], eax
[ebp+var_4], 0
 .text:0040100E
                                   mov
  .text:00401011
                                   спр
.text:00401015
                                           short loc_40102B
                                           offset aSuccessInterne ; "Success: Internet Connection\n"
                                   push
* .text:0040101C
                                   call
                                           sub_40105F
                                           esp, 4
eax, 1
  .text:00401021
                                   add
.text:00401024
.text:00401029
                                   jmp
                                           short loc_40103A
 .text:0040102B
 .text:0040102B
```