Example1.c

The stack frames in this example will be very simple.
Only saved frame pointer (ebp) and saved return addresses (eip).

```
//Example1 - using the stack
//to call subroutines
//New instructions:
//push, pop, call, ret, mov
int sub(){
    return 0xbeef;
}
int main(){
    sub();
    return 0xf00d;
}
```

```
sub:
00401000  push      ebp
00401001  mov       ebp,esp
00401003  mov       eax,0BEEFh
00401008  pop       ebp
00401009  ret
main:
00401010  push      ebp
00401011  mov       ebp,esp
00401013  call      sub (401000h)
00401018  mov       eax,0F00Dh
0040101D  pop       ebp
0040101E  ret
```

Example1.c 1:

EIP = 00401010, but no instruction yet executed

eax	0x003435C0 ⌘
ebp	0x0012FFB8 ⌘
esp	0x0012FF6C ⌘

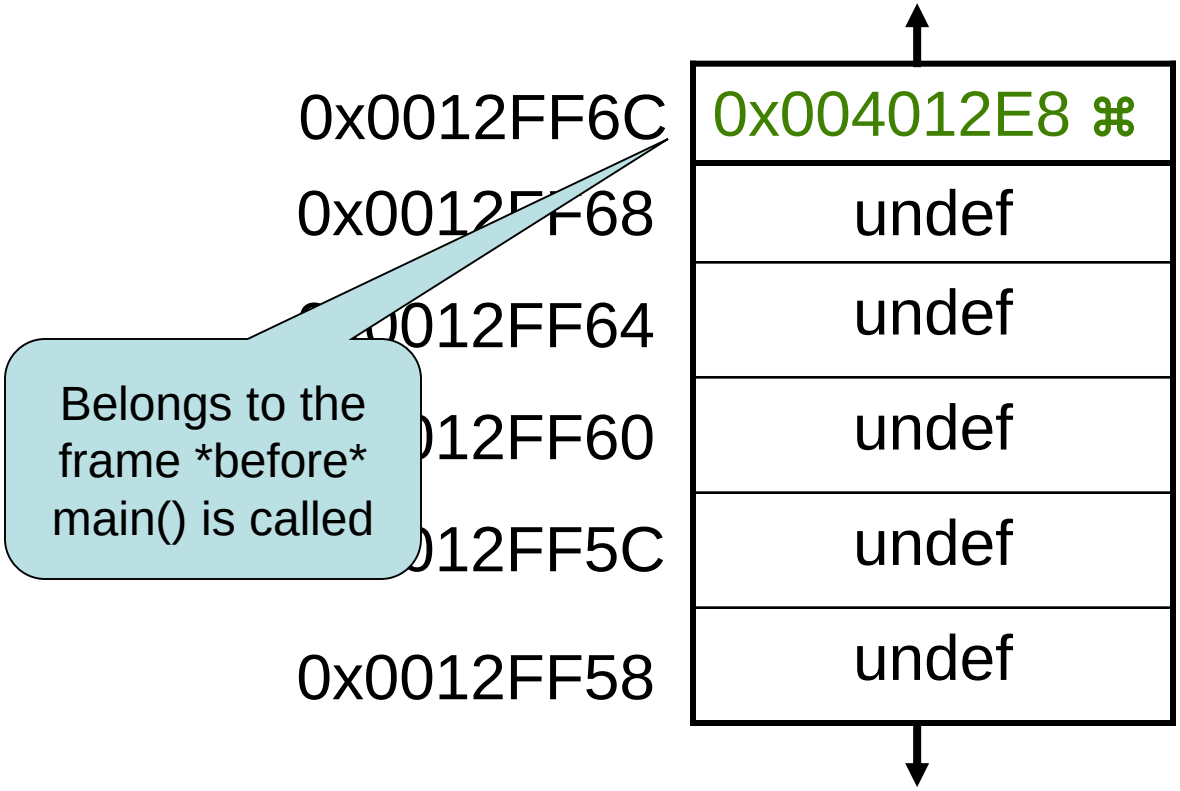
Key:

☒ **executed instruction,**

♍ **modified value**

⌘ **start value**

```
sub:
00401000  push      ebp
00401001  mov       ebp,esp
00401003  mov       eax,0BEEFh
00401008  pop       ebp
00401009  ret
main:
00401010  push      ebp
00401011  mov       ebp,esp
00401013  call      sub (401000h)
00401018  mov       eax,0F00Dh
0040101D  pop       ebp
0040101E  ret
```



Example1.c 2

eax	0x003435C0 ⌘
ebp	0x0012FFB8 ⌘
esp	0x0012FF68 ♍

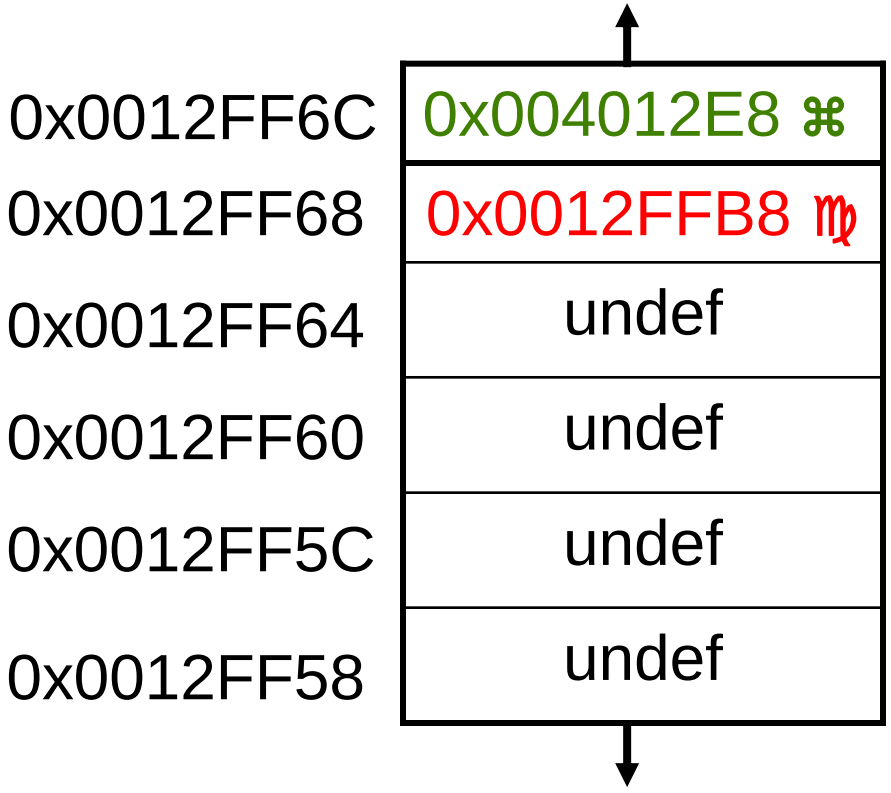
Key:

☒ **executed instruction,**

♍ **modified value**

⌘ **start value**

```
sub:
00401000  push      ebp
00401001  mov       ebp,esp
00401003  mov       eax,0BEEFh
00401008  pop       ebp
00401009  ret
main:
00401010  push      ebp ☒
00401011  mov       ebp,esp
00401013  call      sub (401000h)
00401018  mov       eax,0F00Dh
0040101D  pop       ebp
0040101E  ret
```



Example1.c 3

eax	0x003435C0 ⌘
ebp	0x0012FF68 ♍
esp	0x0012FF68

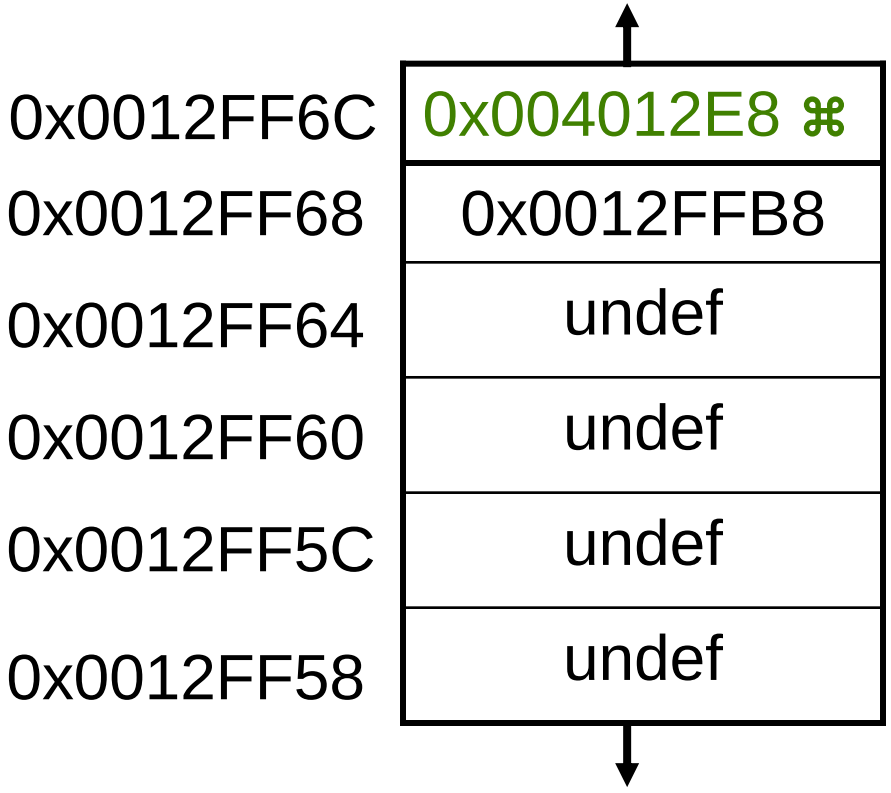
Key:

☒ **executed instruction,**

♍ **modified value**

⌘ **start value**

```
sub:
00401000  push      ebp
00401001  mov       ebp,esp
00401003  mov       eax,0BEEFh
00401008  pop       ebp
00401009  ret
main:
00401010  push      ebp
00401011  mov       ebp,esp ☒
00401013  call      sub (401000h)
00401018  mov       eax,0F00Dh
0040101D  pop       ebp
0040101E  ret
```



Example1.c 4

eax	0x003435C0 ⌘
ebp	0x0012FF68
esp	0x0012FF64 ♍

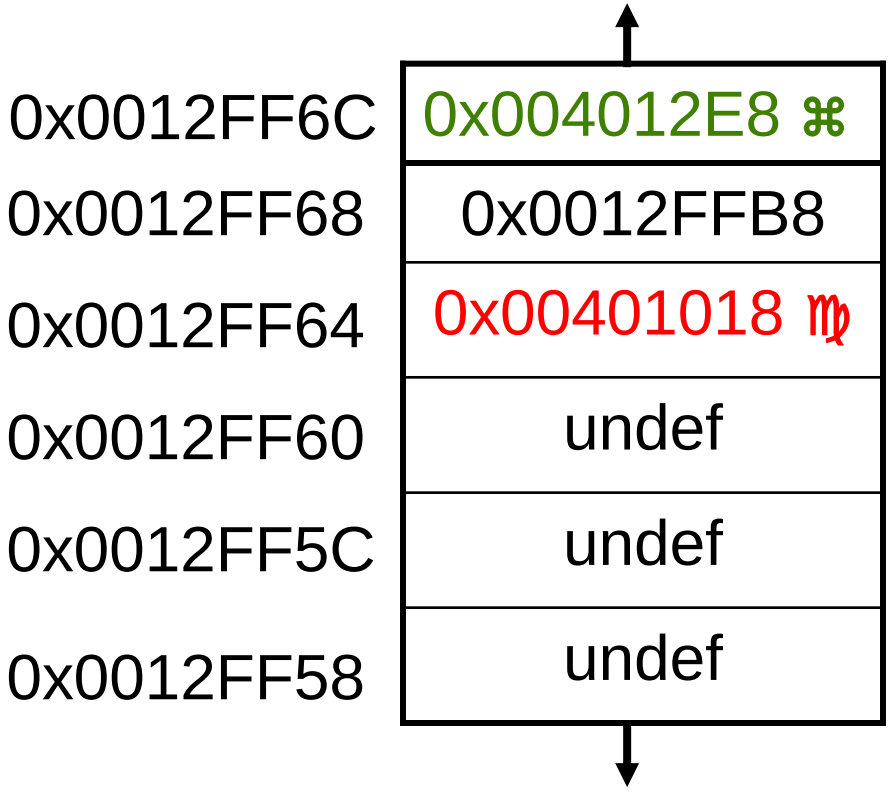
Key:

☒ **executed instruction,**

♍ **modified value**

⌘ **start value**

```
sub:
00401000  push      ebp
00401001  mov       ebp,esp
00401003  mov       eax,0BEEFh
00401008  pop       ebp
00401009  ret
main:
00401010  push      ebp
00401011  mov       ebp,esp
00401013  call      sub (401000h) ☒
00401018  mov       eax,0F00Dh
0040101D  pop       ebp
0040101E  ret
```



Example1.c 5

eax	0x003435C0 ⌘
ebp	0x0012FF68
esp	0x0012FF60 ♍

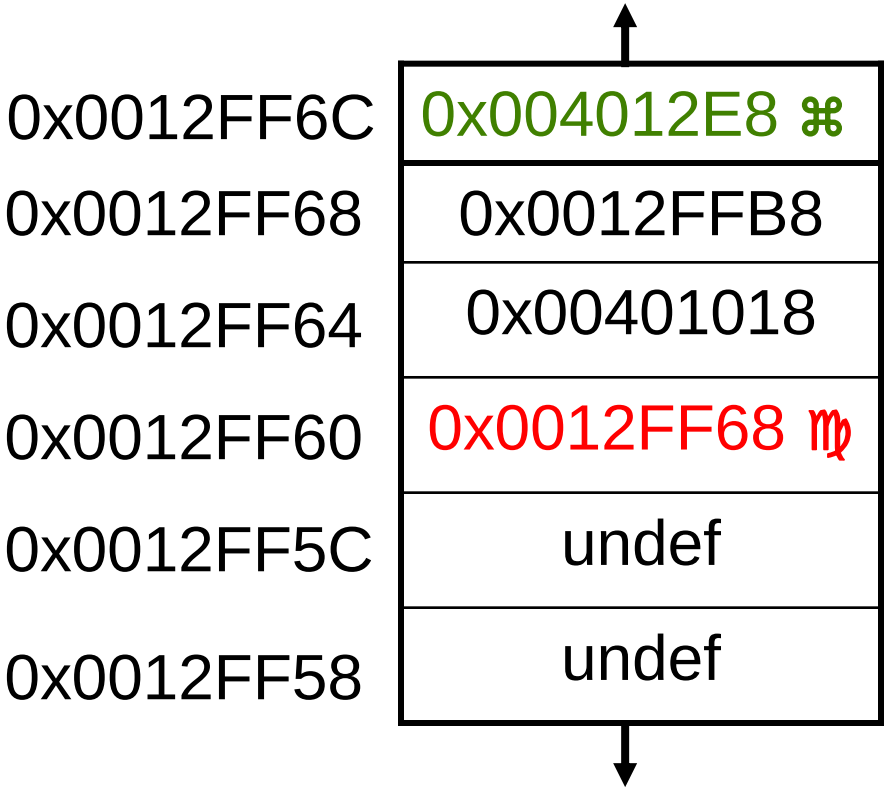
Key:

☒ **executed instruction,**

♍ **modified value**

⌘ **start value**

```
sub:
00401000  push      ebp ☒
00401001  mov       ebp,esp
00401003  mov       eax,0BEEFh
00401008  pop       ebp
00401009  ret
main:
00401010  push      ebp
00401011  mov       ebp,esp
00401013  call      sub (401000h)
00401018  mov       eax,0F00Dh
0040101D  pop       ebp
0040101E  ret
```



Example1.c 6

eax	0x003435C0 ⌘
ebp	0x0012FF60 ♍
esp	0x0012FF60

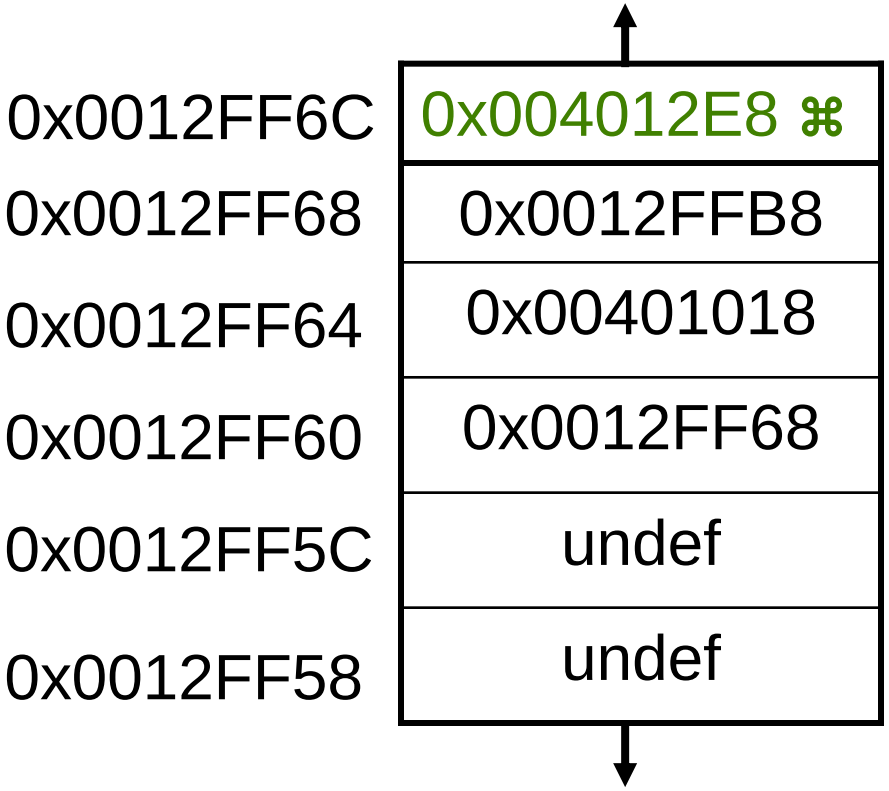
Key:

☒ **executed instruction,**

♍ **modified value**

⌘ **start value**

```
sub:
00401000  push      ebp
00401001  mov       ebp,esp ☒
00401003  mov       eax,0BEEFh
00401008  pop       ebp
00401009  ret
main:
00401010  push      ebp
00401011  mov       ebp,esp
00401013  call      sub (401000h)
00401018  mov       eax,0F00Dh
0040101D  pop       ebp
0040101E  ret
```



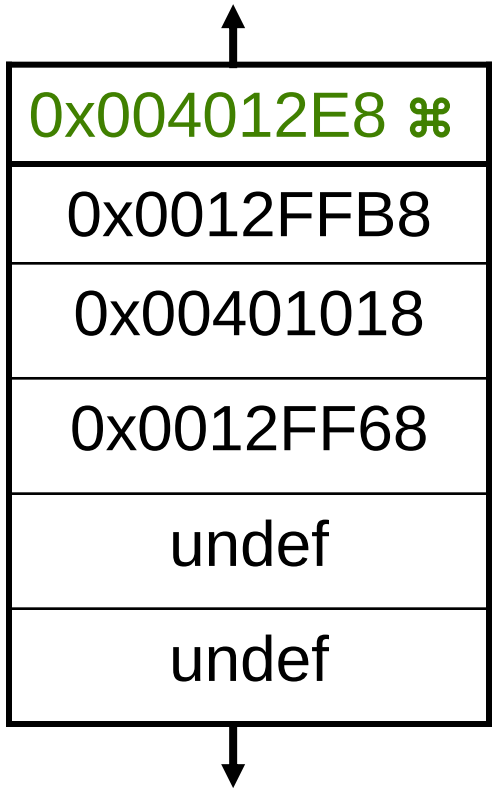
Example1.c 6
STACK FRAME TIME OUT

```
 sub
push    ebp
mov     ebp, esp
mov     eax, 0BEEFh
pop     ebp
retn
main
push    ebp
mov     ebp, esp
call    _sub
mov     eax, 0F00Dh
pop     ebp
retn
```

"Function-before-main"'s frame

main's frame
(saved frame pointer and saved return address)

sub's frame
(only saved frame pointer, because it doesn't call anything else, and doesn't have local variables)



Example1.c 7

eax	0x0000BEEF
ebp	0x0012FF60
esp	0x0012FF60

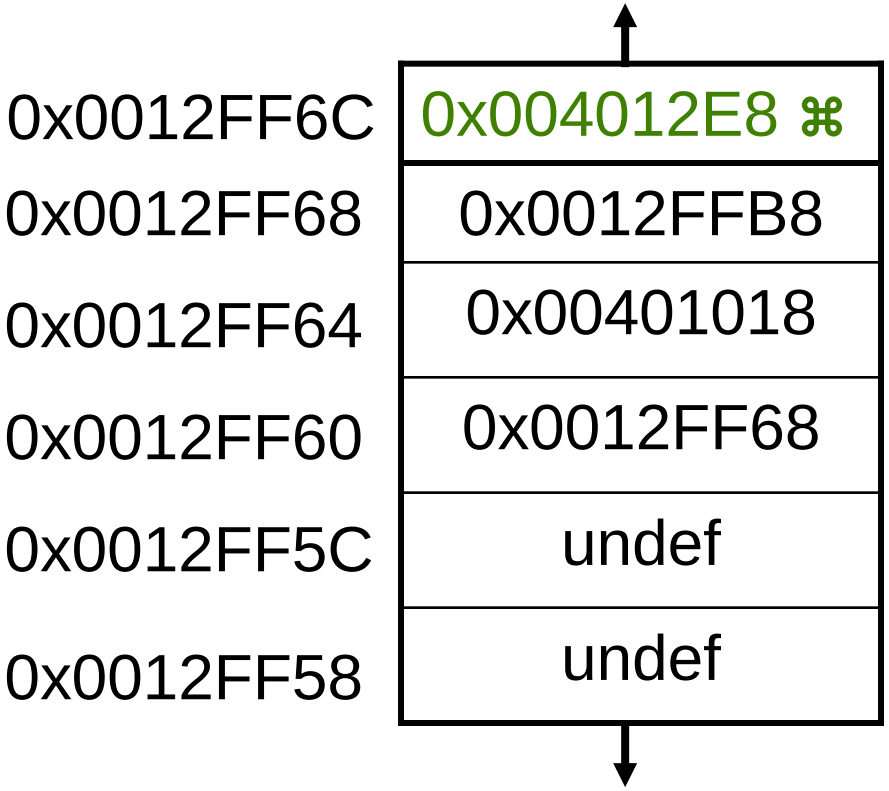
Key:

☒ **executed instruction,**

♍ **modified value**

⌘ **start value**

```
sub:
00401000  push      ebp
00401001  mov       ebp,esp
00401003  mov       eax,0BEEFh ☒
00401008  pop       ebp
00401009  ret
main:
00401010  push      ebp
00401011  mov       ebp,esp
00401013  call      sub (401000h)
00401018  mov       eax,0F00Dh
0040101D  pop       ebp
0040101E  ret
```



Example1.c 8

eax	0x0000BEEF
ebp	0x0012FF68 ♍
esp	0x0012FF64 ♍

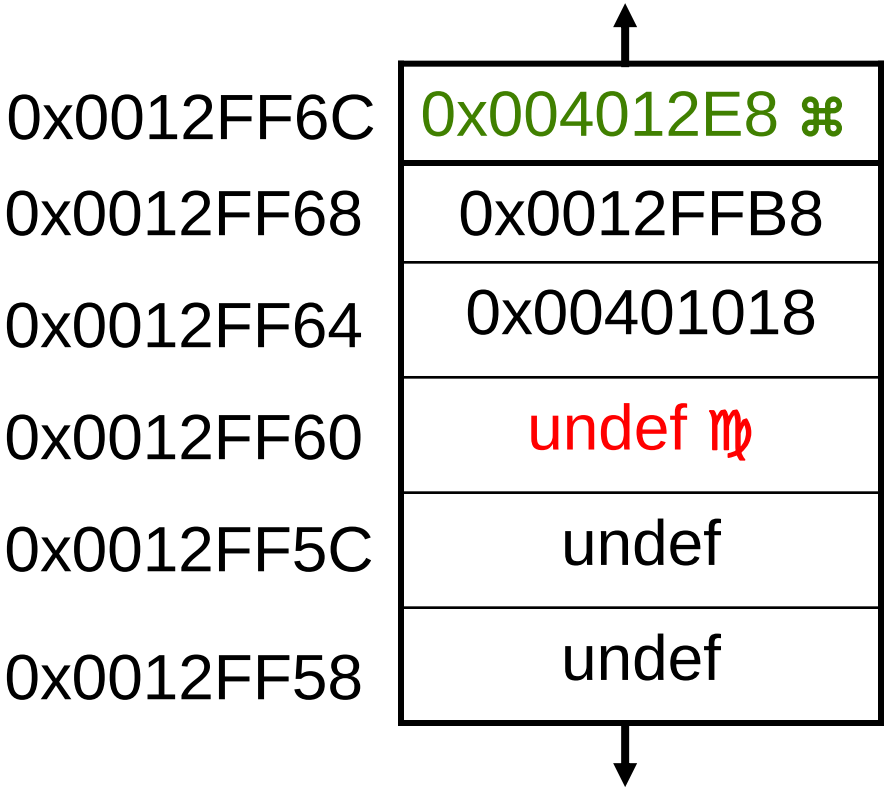
Key:

☒ **executed instruction,**

♍ **modified value**

⌘ **start value**

```
sub:
00401000  push      ebp
00401001  mov       ebp,esp
00401003  mov       eax,0BEEFh
00401008  pop       ebp ☒
00401009  ret
main:
00401010  push      ebp
00401011  mov       ebp,esp
00401013  call      sub (401000h)
00401018  mov       eax,0F00Dh
0040101D  pop       ebp
0040101E  ret
```

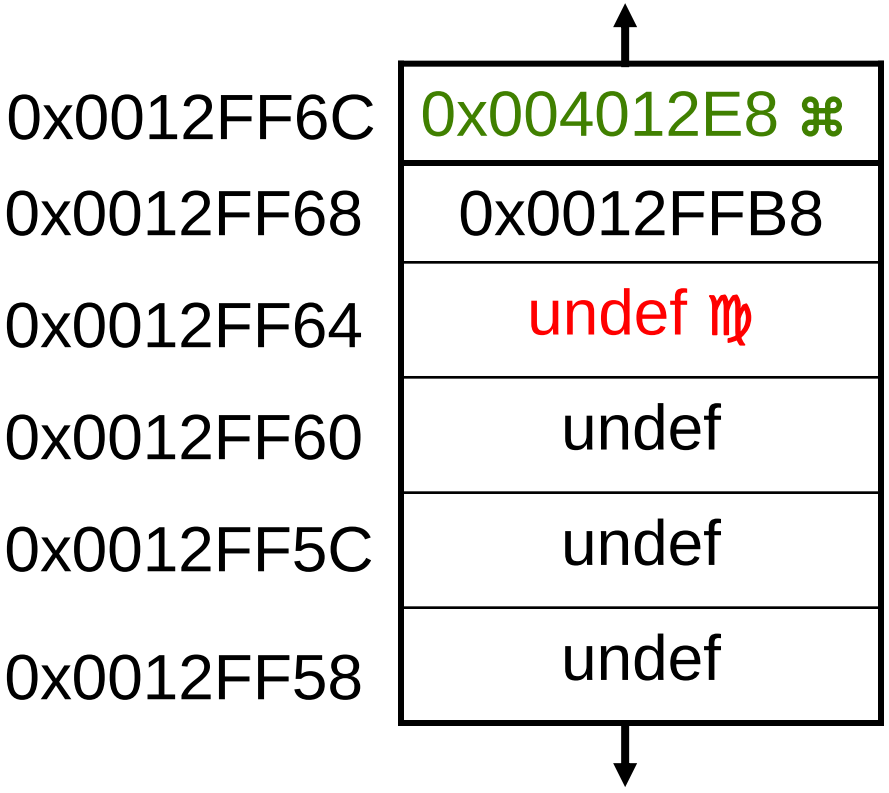


Example1.c 9

eax	0x0000BEEF
ebp	0x0012FF68
esp	0x0012FF68 ♍

Key:
☒ **executed instruction,**
♍ **modified value**
⌘ **start value**

```
sub:
00401000  push      ebp
00401001  mov       ebp,esp
00401003  mov       eax,0BEEFh
00401008  pop       ebp
00401009  ret ☒
main:
00401010  push      ebp
00401011  mov       ebp,esp
00401013  call      sub (401000h)
00401018  mov       eax,0F00Dh
0040101D  pop       ebp
0040101E  ret
```

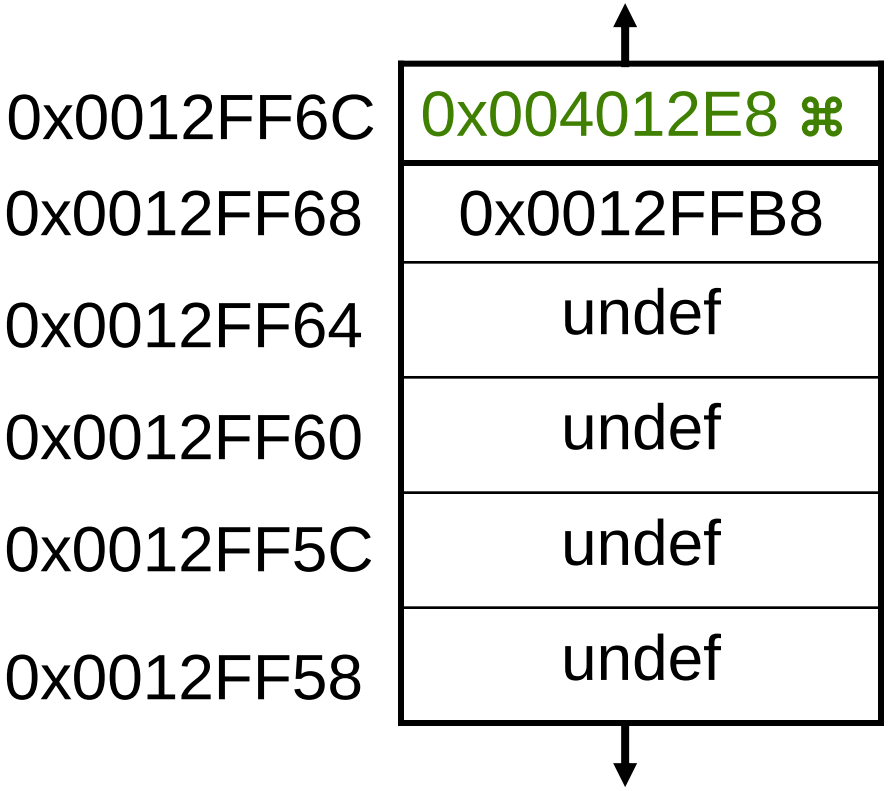


Example1.c 9

eax	0x0000F00D ♍
ebp	0x0012FF68
esp	0x0012FF68

Key:
☒ **executed instruction,**
♍ **modified value**
⌘ **start value**

```
sub:
00401000  push      ebp
00401001  mov       ebp,esp
00401003  mov       eax,0BEEFh
00401008  pop       ebp
00401009  ret
main:
00401010  push      ebp
00401011  mov       ebp,esp
00401013  call      sub (401000h)
00401018  mov       eax,0F00Dh ☒
0040101D  pop       ebp
0040101E  ret
```

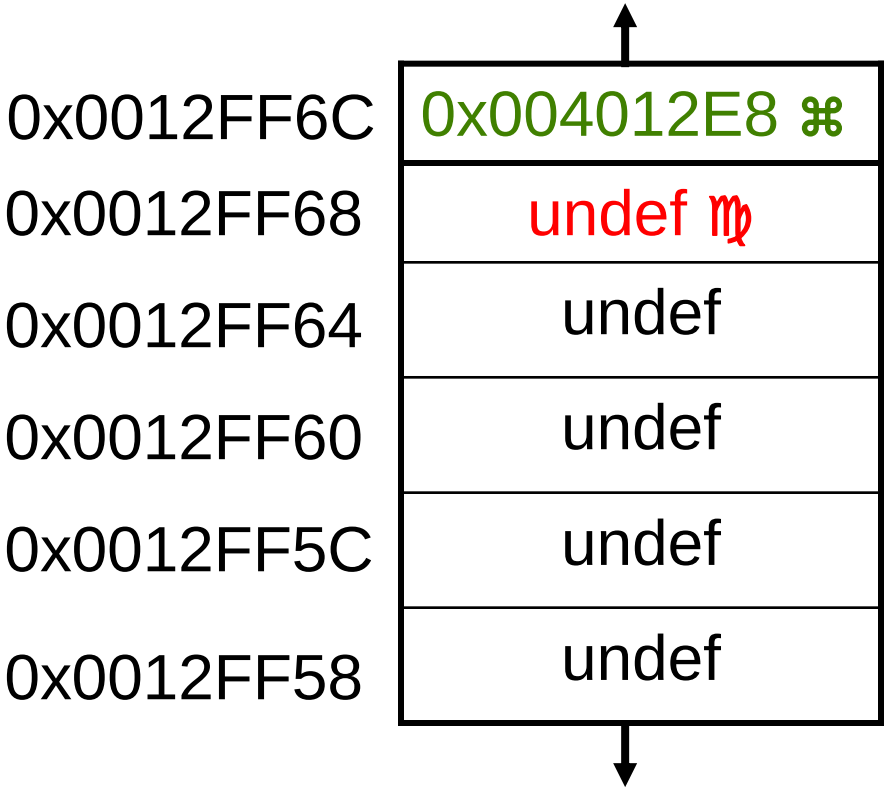


Example1.c 10

eax	0x0000F00D
ebp	0x0012FFB8 ♍
esp	0x0012FF6C ♍

Key:
☒ **executed instruction,**
♍ **modified value**
⌘ **start value**

```
sub:
00401000  push      ebp
00401001  mov       ebp,esp
00401003  mov       eax,0BEEFh
00401008  pop       ebp
00401009  ret
main:
00401010  push      ebp
00401011  mov       ebp,esp
00401013  call      sub (401000h)
00401018  mov       eax,0F00Dh
0040101D  pop       ebp ☒
0040101E  ret
```

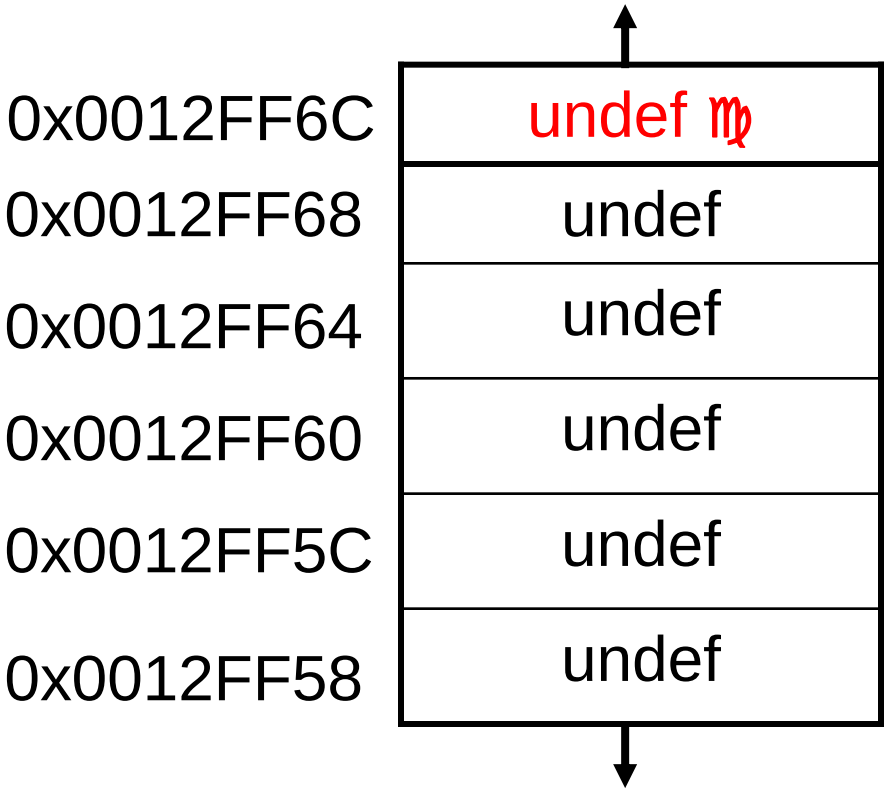


Example1.c 11

eax	0x0000F00D
ebp	0x0012FFB8
esp	0x0012FF70 ♍

Key:
☒ **executed instruction,**
♍ **modified value**
⌘ **start value**

```
sub:
00401000  push      ebp
00401001  mov       ebp,esp
00401003  mov       eax,0BEEFh
00401008  pop       ebp
00401009  ret
main:
00401010  push      ebp
00401011  mov       ebp,esp
00401013  call      sub (401000h)
00401018  mov       eax,0F00Dh
0040101D  pop       ebp
0040101E  ret ☒
```



Execution would continue at the value ret removed from the stack: 0x004012E8