The stack frames in this example will be very simple.

Only saved frame pointer (ebp) and saved return addresses (eip).

```
sub:
//Example1 - using the stack
                                         00401000 push
                                                         ebp
//to call subroutines
                                         00401001 mov
                                                         ebp,esp
//New instructions:
                                         00401003 mov
                                                         eax,0BEEFh
//push, pop, call, ret, mov
                                         00401008 pop
                                                         ebp
                                         00401009 ret
int sub(){
                                         main:
   return 0xbeef;
                                         00401010 push
                                                         ebp
                                         00401011 mov
                                                         ebp,esp
int main(){
                                         00401013 call
                                                        sub (401000h)
   sub();
                                         00401018 mov
                                                         eax,0F00Dh
                                         0040101D pop
                                                         ebp
   return 0xf00d;
                                         0040101E ret
```

#### 

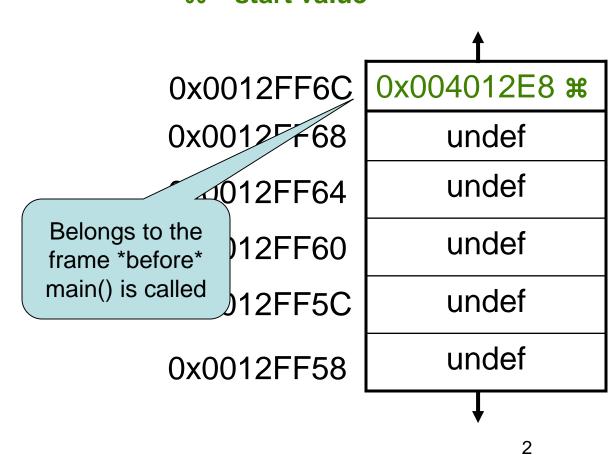
## EIP = 00401010, but no instruction yet executed:

eax	0x003435C0 #
ebp	0x0012FFB8
esp	0x0012FF6C ₩

☑ 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	

cuh.



eax	0x003435C0 ₩
ebp	0x0012FFB8 #
esp	0x0012FF68 <b>M</b>

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

Key:

**x** executed instruction,

**modified value** 

**署 start value** 

0x0012FF6C

0x0012FF68

0x0012FF64

0x0012FF60

0x0012FF5C

0x0012FF58

0x004012E8 #

0x0012FFB8 m

undef

undef

undef

eax	0x003435C0
ebp	0x0012FF68 <b>10</b>
esp	0x0012FF68

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 **区** 

00401013 call sub (401000h)

00401018 mov eax,0F00Dh

0040101D pop ebp

0040101E ret

Key:

**x** executed instruction,

**modified value** 

**業 start value** 

0x0012FF6C

0x0012FF68

0x0012FF64

0x0012FF60

0x0012FF5C

0x0012FF58

0x004012E8 #

0x0012FFB8

undef

undef

undef

eax	0x003435C0 #
ebp	0x0012FF68
esp	0x0012FF64 m/

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

Key:

**x** executed instruction,

**modified value** 

**署 start value** 

0x0012FF6C

0x0012FF68

0x0012FF64

0x0012FF60

0x0012FF5C

0x0012FF58

0x004012E8 #

0x0012FFB8

0x00401018 m

undef

undef

eax	0x003435C0
ebp	0x0012FF68
esp	0x0012FF60 m

#### 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

00401010 push ebp
00401011 mov ebp,esp
00401013 call sub (401000h)
00401018 mov eax,0F00Dh
0040101D pop ebp
0040101E ret

#### Key:

**x** executed instruction,

**modified value** 

**業 start value** 

0x004012E8 # 0x0012FF6C 0x0012FF68 0x0012FFB8 0x00401018 0x0012FF64 0x0012FF68 m 0x0012FF60 undef 0x0012FF5C undef 0x0012FF58

eax	0x003435C0 ₩
ebp	0x0012FF60 m
esp	0x0012FF60

sub:

00401000 push ebp

00401001 mov ebp,esp **区** 

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

Key:

**x** executed instruction,

**modified value** 

**業 start value** 

0x0012FF6C

0x0012FF68

0x0012FF64

0x0012FF60

0x0012FF5C

0x0012FF58

0x004012E8 #

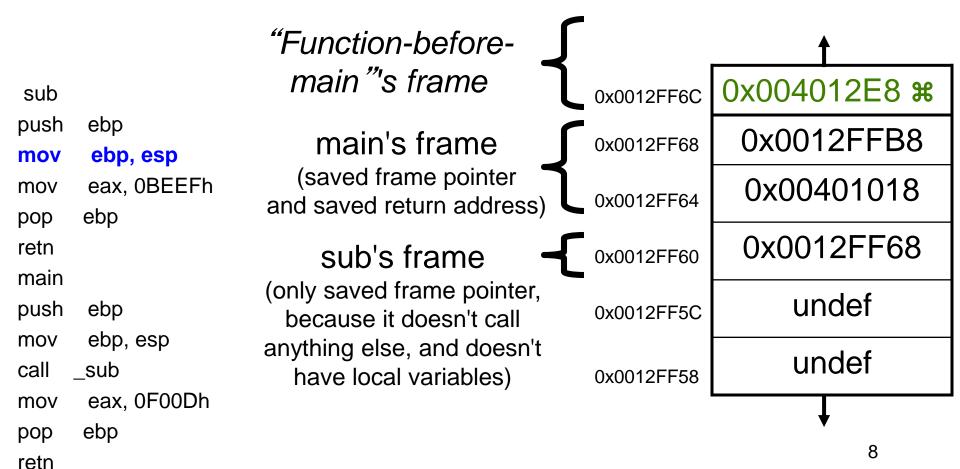
0x0012FFB8

0x00401018

0x0012FF68

undef

# Example1.c 6 STACK FRAME TIME OUT



eax	0x0000BEEF
ebp	0x0012FF60
esp	0x0012FF60

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

Key:

**x** executed instruction,

**modified value** 

**業 start value** 

0x0012FF6C

0x0012FF68

0x0012FF64

0x0012FF60

0x0012FF5C

0x0012FF58

0x004012E8 #

0x0012FFB8

0x00401018

0x0012FF68

undef

eax	0x0000BEEF
ebp	0x0012FF68 m
esp	0x0012FF64 m/

sub:

00401000 push ebp

00401001 mov ebp,esp 00401003 mov eax,0BEEFh

00401003 mov eax,0BLL11

00401009 ret

main:

00401010 push ebp

00401011 mov ebp,esp

00401013 call sub (401000h)

00401018 mov eax,0F00Dh

0040101D pop ebp

0040101E ret

Key:

**x** executed instruction,

**M** modified value

**端** start value

0x0012FF6C

0x0012FF68

0x0012FF64

0x0012FF60

0x0012FF5C

0x0012FF58

0x004012E8 #

0x0012FFB8

0x00401018

undef My

undef

eax	0x0000BEEF
ebp	0x0012FF68
esp	0x0012FF68 m/

sub:

00401000 push ebp 00401001 mov ebp,esp

00401003 mov eax,0BEEFh

00401008 pop ebp

00401009 ret **区** 

main:

00401010 push ebp

00401011 mov ebp,esp

00401013 call sub (401000h)

00401018 mov eax,0F00Dh

0040101D pop ebp

0040101E ret

Key:

**x** executed instruction,

**M** modified value

**光 start value** 

0x0012FF6C

0x0012FF68

0x0012FF64

0x0012FF60

0x0012FF5C

0x0012FF58

0x004012E8 #

0x0012FFB8

undef m

undef

undef

eax	0x0000F00D m
ebp	0x0012FF68
esp	0x0012FF68

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 **区** 

0040101D pop ebp

0040101E ret

Key:

**x** executed instruction,

**modified value** 

**¥** start value

0x0012FF6C

0x0012FF68

0x0012FF64

0x0012FF60

0x0012FF5C

0x0012FF58

0x004012E8 #

0x0012FFB8

undef

undef

undef

eax	0x0000F00D
ebp	0x0012FFB8 m
esp	0x0012FF6C m/

sub:

00401000 push ebp 00401001 mov ebp,esp

00401003 mov eax,0BEEFh

00401008 pop ebp

00401009 ret

00401011 mov

main:

00401010 push ebp

ebp,esp

00401013 call sub (401000h)

00401018 mov eax,0F00Dh

0040101D pop ebp ⊠

0040101E ret

Key:

**x** executed instruction,

**M** modified value

**端** start value

0x0012FF6C

0x0012FF68

0x0012FF64

0x0012FF60

0x0012FF5C

0x0012FF58

0x004012E8 \*\*

undef m

undef

undef

undef

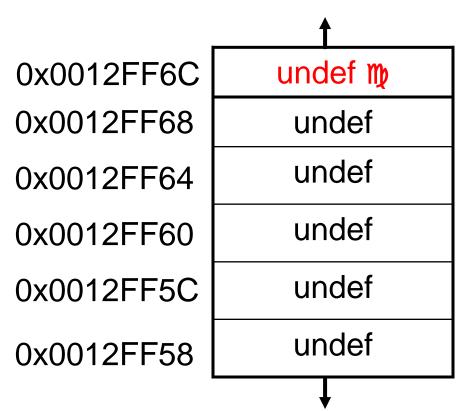
eax	0x0000F00D
ebp	0x0012FFB8
esp	0x0012FF70 m

esp	0x001	0x0012FF70 m		
sub:				
00401000 p	oush	ebp		
00401001 r	nov	ebp,esp		
00401003 r	nov	eax,0BEEFh		
00401008 μ	оор	ebp		

main:
00401010 push ebp
00401011 mov ebp,esp
00401013 call sub (401000h)
00401018 mov eax,0F00Dh
0040101E ret 🔀

00401009 ret

Key:		
X	executed instruction	
m	modified value	
$\mathfrak{H}$	start value	



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