

# x86\_32bit Program Execution

Software Security

Pedro Adão 2022/23

(with Ana Matos & Miguel Pupo Correia)

# Disassemble

```
0x080483f6 int f1(int fx1, int fy1, int fz1){
    int fa1 = 20;
    return fa1;
}

0x08048412 int f(int fx, int fy){
    int fa = 10, fb = 12;
    f1(fx, fy, fa);
    return fb;
}

0x08048439 }

0x08048446 int g(int gx, int gy){
    return gx + gy;
}

0x0804845d int main(){
    int a = 3, b = 5, c = 7;
    f(a,b);
    g(b,c);
    return 0;
}
```

Dump of assembler code for function f1:

```
0x080483f6 <+0>: push    ebp
0x080483f7 <+1>: mov     ebp,esp
0x080483f9 <+3>: sub     esp,0x10
0x080483fc <+6>: call    0x80484a5 <__x86.get_pc_thunk.ax>
0x08048401 <+11>: add     eax,0x1bff
0x08048406 <+16>: mov     DWORD PTR [ebp-0x4],0x14
0x0804840d <+23>: mov     eax,DWORD PTR [ebp-0x4]
0x08048410 <+26>: leave
0x08048411 <+27>: ret
```

Dump of assembler code for function f:

```
0x08048412 <+0>: push    ebp
0x08048413 <+1>: mov     ebp,esp
0x08048415 <+3>: sub     esp,0x10
0x08048418 <+6>: call    0x80484a5 <__x86.get_pc_thunk.ax>
0x0804841d <+11>: add     eax,0x1be3
0x08048422 <+16>: mov     DWORD PTR [ebp-0x4],0xa
0x08048429 <+23>: mov     DWORD PTR [ebp-0x8],0xc
0x08048430 <+30>: push    DWORD PTR [ebp-0x4]
0x08048433 <+33>: push    DWORD PTR [ebp+0xc]
0x08048436 <+36>: push    DWORD PTR [ebp+0x8]
0x08048439 <+39>: call    0x80483f6 <f1>
0x0804843e <+44>: add     esp,0xc
0x08048441 <+47>: mov     eax,DWORD PTR [ebp-0x8]
0x08048444 <+50>: leave
0x08048445 <+51>: ret
```

# Disassemble

```
0x080483f6 int f1(int fx1, int fy1, int fz1){
    int fa1 = 20;
    return fa1;
}

0x08048412 int f(int fx, int fy){
    int fa = 10, fb = 12;
    f1(fx, fy, fa);
    return fb;
}

0x08048439

0x08048446 int g(int gx, int gy){
    return gx + gy;
}

0x0804845d int main(){
    int a = 3, b = 5, c = 7;
    f(a,b);
    g(b,c);
    return 0;
}
```

Dump of assembler code for function f1:

```
0x080483f6 <+0>: push    ebp
0x080483f7 <+1>: mov     ebp,esp
0x080483f9 <+3>: sub     esp,0x10
0x080483fc <+6>: call    0x80484a5 <__x86.get_pc_thunk.ax>
0x08048401 <+11>: add     eax,0x1bff
0x08048406 <+16>: mov     DWORD PTR [ebp-0x4],0x14
0x0804840d <+23>: mov     eax,DWORD PTR [ebp-0x4]
0x08048410 <+26>: leave
0x08048411 <+27>: ret
```

Dump of assembler code for function f:

```
0x08048412 <+0>: push    ebp
0x08048413 <+1>: mov     ebp,esp
0x08048415 <+3>: sub     esp,0x10
0x08048418 <+6>: call    0x80484a5 <__x86.get_pc_thunk.ax>
0x0804841d <+11>: add     eax,0x1be3
0x08048422 <+16>: mov     DWORD PTR [ebp-0x4],0xa
0x08048429 <+23>: mov     DWORD PTR [ebp-0x8],0xc
0x08048430 <+30>: push    DWORD PTR [ebp-0x4]
0x08048433 <+33>: push    DWORD PTR [ebp+0xc]
0x08048436 <+36>: push    DWORD PTR [ebp+0x8]
0x08048439 <+39>: call    0x80483f6 <f1>
0x0804843e <+44>: add     esp,0xc
0x08048441 <+47>: mov     eax,DWORD PTR [ebp-0x8]
0x08048444 <+50>: leave
0x08048445 <+51>: ret
```

# Disassemble

```
0x080483f6 int f1(int fx1, int fy1, int fz1){
    int fa1 = 20;
    return fa1;
}

0x08048412 int f(int fx, int fy){
    int fa = 10, fb = 12;
    f1(fx, fy, fa);
    return fb;
}

0x08048439

0x08048446 int g(int gx, int gy){
    return gx + gy;
}

0x0804845d int main(){
    int a = 3, b = 5, c = 7;
    f(a,b);
    g(b,c);
    return 0;
}
```

Dump of assembler code for function g:

```
0x08048446 <+0>: push    ebp
0x08048447 <+1>: mov     ebp,esp
0x08048449 <+3>: call    0x80484a5 <__x86.get_pc_thunk.ax>
0x0804844e <+8>: add     eax,0x1bb2
0x08048453 <+13>: mov     edx,DWORD PTR [ebp+0x8]
0x08048456 <+16>: mov     eax,DWORD PTR [ebp+0xc]
0x08048459 <+19>: add     eax,edx
0x0804845b <+21>: pop     ebp
0x0804845c <+22>: ret
```

Dump of assembler code for function main:

```
0x0804845d <+0>: push    ebp
0x0804845e <+1>: mov     ebp,esp
0x08048460 <+3>: sub     esp,0x10
0x08048463 <+6>: call    0x80484a5 <__x86.get_pc_thunk.ax>
0x08048468 <+11>: add     eax,0x1b98
0x0804846d <+16>: mov     DWORD PTR [ebp-0x4],0x3
0x08048474 <+23>: mov     DWORD PTR [ebp-0x8],0x5
0x0804847b <+30>: mov     DWORD PTR [ebp-0xc],0x7
0x08048482 <+37>: push    DWORD PTR [ebp-0x8]
0x08048485 <+40>: push    DWORD PTR [ebp-0x4]
0x08048488 <+43>: call    0x8048412 <f>
0x0804848d <+48>: add     esp,0x8
0x08048490 <+51>: push    DWORD PTR [ebp-0xc]
0x08048493 <+54>: push    DWORD PTR [ebp-0x8]
0x08048496 <+57>: call    0x8048446 <g>
0x0804849b <+62>: add     esp,0x8
0x0804849e <+65>: mov     eax,0x0
0x080484a3 <+70>: leave
0x080484a4 <+71>: ret
```

# Disassemble

```
0x080483f6 int f1(int fx1, int fy1, int fz1){
    int fa1 = 20;
    return fa1;
}

0x08048412 int f(int fx, int fy){
    int fa = 10, fb = 12;
    f1(fx, fy, fa);
    return fb;
}

0x08048446 int g(int gx, int gy){
    return gx + gy;
}

0x0804845d int main(){
    int a = 3, b = 5, c = 7;
    f(a,b);
    g(b,c);
    return 0;
}
```

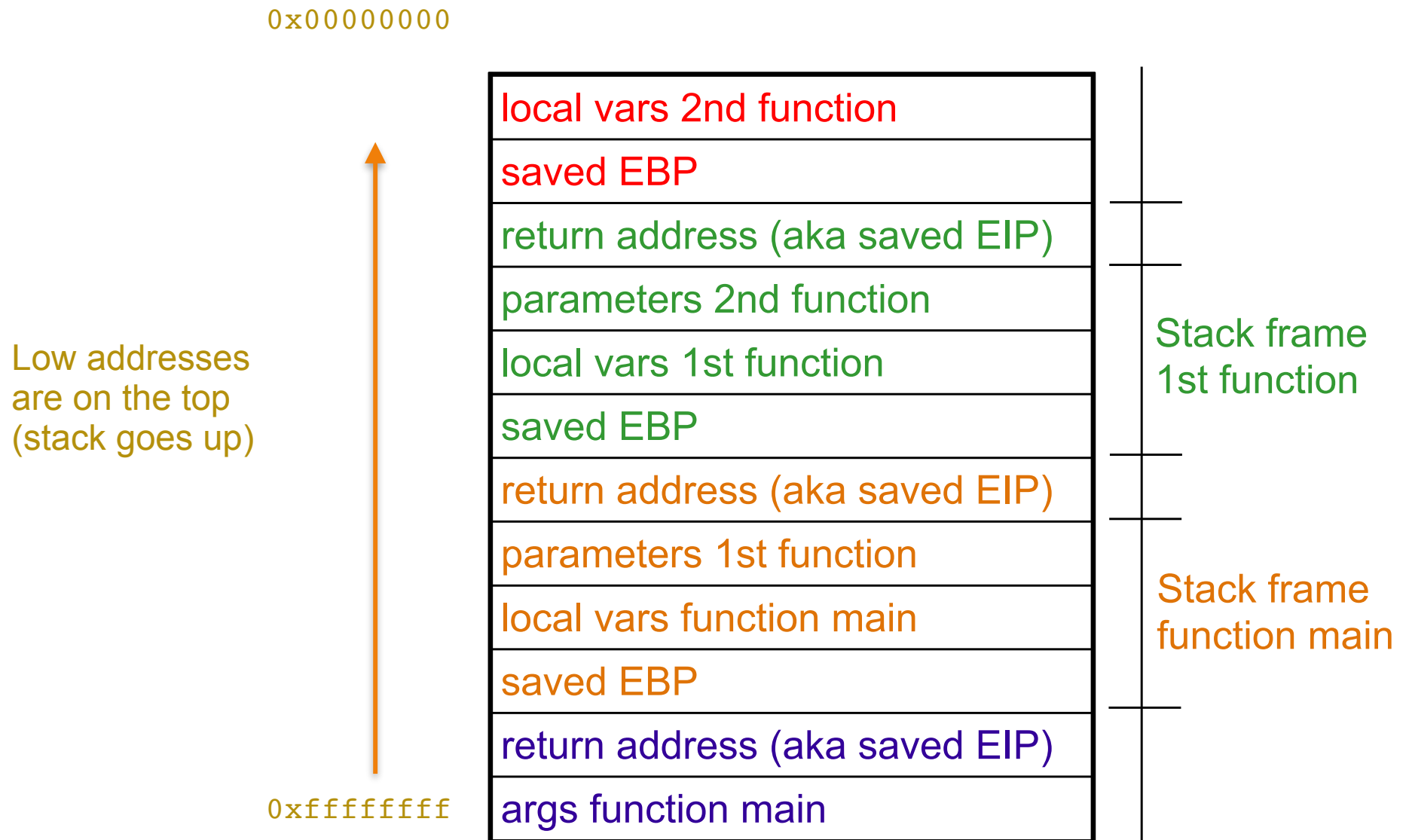
Dump of assembler code for function g:

```
0x08048446 <+0>: push    ebp
0x08048447 <+1>: mov     ebp,esp
0x08048449 <+3>: call    0x80484a5 <__x86.get_pc_thunk.ax>
0x0804844e <+8>: add     eax,0x1bb2
0x08048453 <+13>: mov     edx,DWORD PTR [ebp+0x8]
0x08048456 <+16>: mov     eax,DWORD PTR [ebp+0xc]
0x08048459 <+19>: add     eax,edx
0x0804845b <+21>: pop     ebp
0x0804845c <+22>: ret
```

Dump of assembler code for function main:

```
0x0804845d <+0>: push    ebp
0x0804845e <+1>: mov     ebp,esp
0x08048460 <+3>: sub     esp,0x10
0x08048463 <+6>: call    0x80484a5 <__x86.get_pc_thunk.ax>
0x08048468 <+11>: add     eax,0x1b98
0x0804846d <+16>: mov     DWORD PTR [ebp-0x4],0x3
0x08048474 <+23>: mov     DWORD PTR [ebp-0x8],0x5
0x0804847b <+30>: mov     DWORD PTR [ebp-0xc],0x7
0x08048482 <+37>: push    DWORD PTR [ebp-0x8]
0x08048485 <+40>: push    DWORD PTR [ebp-0x4]
0x08048488 <+43>: call    0x8048412 <f>
0x0804848d <+48>: add     esp,0x8
0x08048490 <+51>: push    DWORD PTR [ebp-0xc]
0x08048493 <+54>: push    DWORD PTR [ebp-0x8]
0x08048496 <+57>: call    0x8048446 <g>
0x0804849b <+62>: add     esp,0x8
0x0804849e <+65>: mov     eax,0x0
0x080484a3 <+70>: leave
0x080484a4 <+71>: ret
```

# Stack Layout



# Program Execution

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

**We start with main**

# Program Execution

```
0x080483f6 int f1(int fx1, int fy1, int fz1){  
    int fa1 = 20;  
    return fa1;  
}
```

```
0x08048412 int f(int fx, int fy){  
    int fa = 10, fb = 12;  
0x08048439    f1(fx, fy, fa);  
    return fb;  
}
```

```
0x08048446 int g(int gx, int gy){  
    return gx + gy;  
}
```

```
0x0804845d int main(){  
    int a = 3, b = 5, c = 7;  
0x08048488    f(a,b);  
0x08048496    g(b,c);  
    return 0;  
}
```

**We start with main**

EBP

0xffffd5e8



# Program Execution

```
0x080483f6 int f1(int fx1, int fy1, int fz1){  
    int fa1 = 20;  
    return fa1;  
}
```

```
0x08048412 int f(int fx, int fy){  
    int fa = 10, fb = 12;  
    f1(fx, fy, fa);  
    return fb;  
}
```

```
0x08048446 int g(int gx, int gy){  
    return gx + gy;  
}
```

```
0x0804845d int main(){  
    int a = 3, b = 5, c = 7;  
    f(a,b);  
    g(b,c);  
    return 0;  
}
```

**Next we push the  
local variables of main  
(in order)**

EBP

0xffffd5e8

# Program Execution

```
0x080483f6 int f1(int fx1, int fy1, int fz1){
    int fa1 = 20;
    return fa1;
}
```

```
0x08048412 int f(int fx, int fy){
    int fa = 10, fb = 12;
0x08048439 f1(fx, fy, fa);
    return fb;
}
```

```
0x08048446 int g(int gx, int gy){
    return gx + gy;
}
```

```
0x0804845d int main(){
    int a = 3, b = 5, c = 7;
0x08048488 f(a,b);
0x08048496 g(b,c);
    return 0;
}
```

**Next we push the  
local variables of main  
(in order)**

EBP

0xffffd5e4

3

0xffffd5e8

# Program Execution

```
0x080483f6 int f1(int fx1, int fy1, int fz1){
    int fa1 = 20;
    return fa1;
}
```

```
0x08048412 int f(int fx, int fy){
    int fa = 10, fb = 12;
0x08048439 f1(fx, fy, fa);
    return fb;
}
```

```
0x08048446 int g(int gx, int gy){
    return gx + gy;
}
```

```
0x0804845d int main(){
    int a = 3, b = 5, c = 7;
0x08048488 f(a,b);
0x08048496 g(b,c);
    return 0;
}
```

**Next we push the  
local variables of main  
(in order)**

EBP

0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

```
0x080483f6 int f1(int fx1, int fy1, int fz1){
    int fa1 = 20;
    return fa1;
}
```

```
0x08048412 int f(int fx, int fy){
    int fa = 10, fb = 12;
0x08048439 f1(fx, fy, fa);
    return fb;
}
```

```
0x08048446 int g(int gx, int gy){
    return gx + gy;
}
```

```
0x0804845d int main(){
    int a = 3, b = 5, c = 7;
0x08048488 f(a,b);
0x08048496 g(b,c);
    return 0;
}
```

**Next we push the  
local variables of main  
(in order)**

0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

EBP



# Program Execution

```

0x080483f6 int f1(int fx1, int fy1, int fz1){
           int fa1 = 20;
           return fa1;
           }

```

```

0x08048412 int f(int fx, int fy){
           int fa = 10, fb = 12;
0x08048439 f1(fx, fy, fa);
           return fb;
           }

```

```

0x08048446 int g(int gx, int gy){
           return gx + gy;
           }

```

```

0x0804845d int main(){
           int a = 3, b = 5, c = 7;
           f(a,b);
0x08048488 g(b,c);
0x08048496 return 0;
           }

```

**Before calling function `f`  
push the parameters of `f`  
(in reverse order)**

0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

EBP

# Program Execution

```
0x080483f6 int f1(int fx1, int fy1, int fz1){  
    int fa1 = 20;  
    return fa1;  
}
```

```
0x08048412 int f(int fx, int fy){  
    int fa = 10, fb = 12;  
    f1(fx, fy, fa);  
    return fb;  
}
```

```
0x08048446 int g(int gx, int gy){  
    return gx + gy;  
}
```

```
0x0804845d int main(){  
    int a = 3, b = 5, c = 7;  
    f(a,b);  
    g(b,c);  
    return 0;  
}
```

**Before calling function `f`  
push the parameters of `f`  
(in reverse order)**

0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

EBP

# Program Execution

```
0x080483f6 int f1(int fx1, int fy1, int fz1){
    int fa1 = 20;
    return fa1;
}
```

```
0x08048412 int f(int fx, int fy){
    int fa = 10, fb = 12;
0x08048439 f1(fx, fy, fa);
    return fb;
}
```

```
0x08048446 int g(int gx, int gy){
    return gx + gy;
}
```

```
0x0804845d int main(){
    int a = 3, b = 5, c = 7;
    f(a,b);
0x08048488 g(b,c);
0x08048496 return 0;
}
```

**Before calling function `f`  
push the parameters of `f`  
(in reverse order)**

0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

EBP

# Program Execution

```
0x080483f6 int f1(int fx1, int fy1, int fz1){
            int fa1 = 20;
            return fa1;
            }
```

```
0x08048412 int f(int fx, int fy){
            int fa = 10, fb = 12;
0x08048439 f1(fx, fy, fa);
            return fb;
            }
```

```
0x08048446 int g(int gx, int gy){
            return gx + gy;
            }
```

```
0x0804845d int main(){
            int a = 3, b = 5, c = 7;
            f(a,b);
0x08048488 g(b,c);
0x08048496 return 0;
            }
```

**Before calling function `f`  
push the parameters of `f`  
(in reverse order)**

0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

EBP

0xffffd5e8



# Program Execution

```
0x080483f6 int f1(int fx1, int fy1, int fz1){  
    int fa1 = 20;  
    return fa1;  
}
```

```
0x08048412 int f(int fx, int fy){  
    int fa = 10, fb = 12;  
    f1(fx, fy, fa);  
    return fb;  
}
```

```
0x08048446 int g(int gx, int gy){  
    return gx + gy;  
}
```

```
0x0804845d int main(){  
    int a = 3, b = 5, c = 7;  
    f(a,b);  
    g(b,c);  
    return 0;  
}
```

And the address of `main`  
where to continue  
when `f` finishes

0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

EBP



0xffffd5e8

# Program Execution

```

0x080483f6 int f1(int fx1, int fy1, int fz1){
            int fa1 = 20;
            return fa1;
        }

```

```

0x08048412 int f(int fx, int fy){
            int fa = 10, fb = 12;
0x08048439 f1(fx, fy, fa);
            return fb;
        }

```

```

0x08048446 int g(int gx, int gy){
            return gx + gy;
        }

```

```

0x0804845d int main(){
            int a = 3, b = 5, c = 7;
0x08048488 f(a,b);
0x08048496 g(b,c);
            return 0;
        }

```

And the address of `main`  
where to continue  
when `f` finishes

0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

EBP

# Program Execution

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

**When entering f  
push the address  
of EBP of main**

0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

EBP



0xffffd5e8

# Program Execution

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

**When entering f  
push the address  
of EBP of main**

0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

EBP



# Program Execution

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

And set the  
new EBP of f

0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

EBP



0xffffd5e8

# Program Execution

```

0x080483f6 int f1(int fx1, int fy1, int fz1){
            int fa1 = 20;
            return fa1;
        }
    
```

```

0x08048412 int f(int fx, int fy){
            int fa = 10, fb = 12;
0x08048439 f1(fx, fy, fa);
            return fb;
        }
    
```

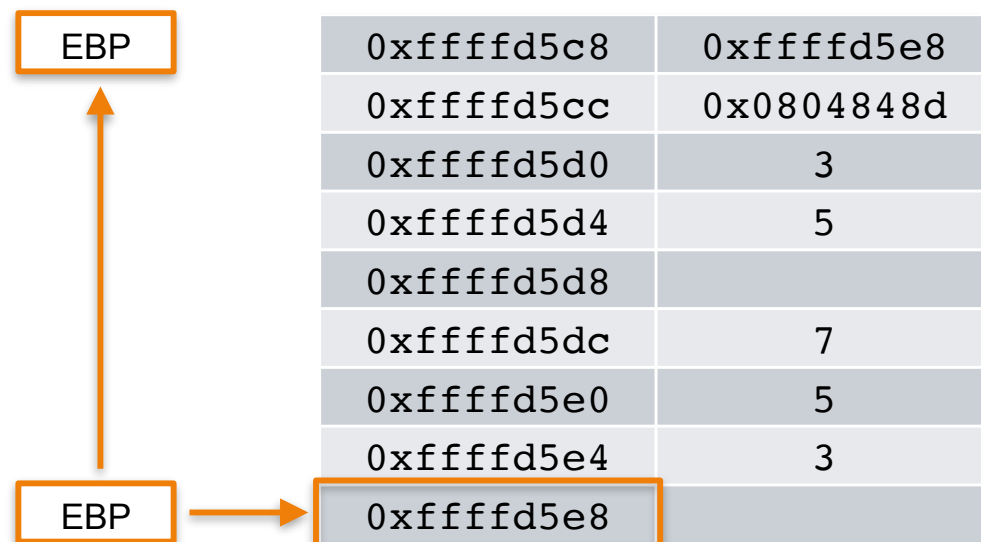
```

0x08048446 int g(int gx, int gy){
            return gx + gy;
        }
    
```

```

0x0804845d int main(){
            int a = 3, b = 5, c = 7;
0x08048488 f(a,b);
0x08048496 g(b,c);
            return 0;
        }
    
```

And set the  
new EBP of f



# Program Execution

```

0x080483f6 int f1(int fx1, int fy1, int fz1){
           int fa1 = 20;
           return fa1;
           }

0x08048412 int f(int fx, int fy){
           int fa = 10, fb = 12;
0x08048439 f1(fx, fy, fa);
           return fb;
           }

0x08048446 int g(int gx, int gy){
           return gx + gy;
           }

0x0804845d int main(){
           int a = 3, b = 5, c = 7;
0x08048488 f(a,b);
0x08048496 g(b,c);
           return 0;
           }

```

And set the  
new EBP of f

EBP

0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

Next we push the  
local variables of **f**  
(in order)

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

EBP

0xffffd5c8

0xffffd5e8

0xffffd5cc

0x0804848d

0xffffd5d0

3

0xffffd5d4

5

0xffffd5d8

0xffffd5dc

7

0xffffd5e0

5

0xffffd5e4

3

0xffffd5e8



# Program Execution

```

0x080483f6 int f1(int fx1, int fy1, int fz1){
            int fa1 = 20;
            return fa1;
        }

0x08048412 int f(int fx, int fy){
0x08048439     int fa = 10, fb = 12;
            f1(fx, fy, fa);
            return fb;
        }

0x08048446 int g(int gx, int gy){
            return gx + gy;
        }

0x0804845d int main(){
            int a = 3, b = 5, c = 7;
0x08048488     f(a,b);
0x08048496     g(b,c);
            return 0;
        }

```

Next we push the  
local variables of f  
(in order)

EBP

0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

```

0x080483f6 int f1(int fx1, int fy1, int fz1){
           int fa1 = 20;
           return fa1;
           }

0x08048412 int f(int fx, int fy){
           int fa = 10, fb = 12;
0x08048439 f1(fx, fy, fa);
           return fb;
           }

0x08048446 int g(int gx, int gy){
           return gx + gy;
           }

0x0804845d int main(){
           int a = 3, b = 5, c = 7;
0x08048488 f(a,b);
0x08048496 g(b,c);
           return 0;
           }

```

Next we push the  
local variables of f  
(in order)

EBP

0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

And call function f1

pushing the parameters of f1  
(in reverse order)

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

EBP

0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

And call function f1

pushing the parameters of f1  
(in reverse order)

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

EBP

0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

And call function f1

pushing the parameters of f1  
(in reverse order)

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

EBP

0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

And call function f1

pushing the parameters of f1  
(in reverse order)

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

EBP

0xffffd5b4	5
0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

And call function f1

pushing the parameters of f1  
(in reverse order)

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

EBP

0xffffd5b0	3
0xffffd5b4	5
0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

And the address of **f**  
where to continue  
when **f1** finishes

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

EBP



0xffffd5b0	3
0xffffd5b4	5
0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	



# Program Execution

And the address of **f**  
where to continue  
when **f1** finishes

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

EBP

0xffffd5ac	0x0804843e
0xffffd5b0	3
0xffffd5b4	5
0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

When entering f1  
push the address  
of EBP of f

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

EBP



0xffffd5ac	0x0804843e
0xffffd5b0	3
0xffffd5b4	5
0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

When entering f1  
push the address  
of EBP of f

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

EBP



0xffffd5a8	0xffffd5c8
0xffffd5ac	0x0804843e
0xffffd5b0	3
0xffffd5b4	5
0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

And set the  
new EBP of f1

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

EBP



0xffffd5ac	0x0804843e
0xffffd5b0	3
0xffffd5b4	5
0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

And set the  
new EBP of f1

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

EBP

EBP

0xffffd5a8	0xffffd5c8
0xffffd5ac	0x0804843e
0xffffd5b0	3
0xffffd5b4	5
0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

And set the  
new EBP of f1

0x080483f6	<code>int f1(int fx1, int fy1, int fz1){</code>
	<code>int fa1 = 20;</code>
	<code>return fa1;</code>
	<code>}</code>
0x08048412	<code>int f(int fx, int fy){</code>
	<code>int fa = 10, fb = 12;</code>
0x08048439	<code>f1(fx, fy, fa);</code>
	<code>return fb;</code>
	<code>}</code>
0x08048446	<code>int g(int gx, int gy){</code>
	<code>return gx + gy;</code>
	<code>}</code>
0x0804845d	<code>int main(){</code>
	<code>int a = 3, b = 5, c = 7;</code>
0x08048488	<code>f(a,b);</code>
0x08048496	<code>g(b,c);</code>
	<code>return 0;</code>
	<code>}</code>

EBP



0xffffd5a8	0xffffd5c8
0xffffd5ac	0x0804843e
0xffffd5b0	3
0xffffd5b4	5
0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

Next we push the  
local variables of f1  
(in order)

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

EBP

0xffffd5a8

0xffffd5c8

0xffffd5ac

0x0804843e

0xffffd5b0

3

0xffffd5b4

5

0xffffd5b8

10

0xffffd5bc

0xffffd5c0

12

0xffffd5c4

10

0xffffd5c8

0xffffd5e8

0xffffd5cc

0x0804848d

0xffffd5d0

3

0xffffd5d4

5

0xffffd5d8

0xffffd5dc

7

0xffffd5e0

5

0xffffd5e4

3

0xffffd5e8

# Program Execution

Next we push the  
local variables of f1  
(in order)

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

EBP

0xffffd5a0	
0xffffd5a4	20
0xffffd5a8	0xffffd5c8
0xffffd5ac	0x0804843e
0xffffd5b0	3
0xffffd5b4	5
0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	



# Program Execution

When f1 returns

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

EBP

0xffffd5a0	
0xffffd5a4	20
0xffffd5a8	0xffffd5c8
0xffffd5ac	0x0804843e
0xffffd5b0	3
0xffffd5b4	5
0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Exec

Resets the previous EBP

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

EBP

0xffffd5a0	
0xffffd5a4	20
0xffffd5a8	0xffffd5c8
0xffffd5ac	0x0804843e
0xffffd5b0	3
0xffffd5b4	5
0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Exec

Resets the previous EBP

```

0x080483f6 int f1(int fx1, int fy1, int fz1){
           int fa1 = 20;
           return fa1;
           }

0x08048412 int f(int fx, int fy){
           int fa = 10, fb = 12;
0x08048439 f1(fx, fy, fa);
           return fb;
           }

0x08048446 int g(int gx, int gy){
           return gx + gy;
           }

0x0804845d int main(){
           int a = 3, b = 5, c = 7;
0x08048488 f(a,b);
0x08048496 g(b,c);
           return 0;
           }

```

EBP

EBP

0xffffd5a0	
0xffffd5a4	20
0xffffd5a8	0xffffd5c8
0xffffd5ac	0x0804843e
0xffffd5b0	3
0xffffd5b4	5
0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Exec

Resets the previous EBP

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

EBP

0xffffd5a0	
0xffffd5a4	20
0xffffd5a8	0xffffd5c8
0xffffd5ac	0x0804843e
0xffffd5b0	3
0xffffd5b4	5
0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution Continues where it stopped in f

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

EBP

0xffffd5a0	
0xffffd5a4	20
0xffffd5a8	0xffffd5c8
0xffffd5ac	0x0804843e
0xffffd5b0	3
0xffffd5b4	5
0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

And the frame of f1  
Becomes unused

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

EBP

0xffffd5a0	
0xffffd5a4	20
0xffffd5a8	0xffffd5c8
0xffffd5ac	0x0804843e
0xffffd5b0	3
0xffffd5b4	5
0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

And the frame of f1  
Becomes unused

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

EBP

0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

When f returns

EBP

0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	



# Program Execution

When f returns

```

0x080483f6 int f1(int fx1, int fy1, int fz1){
           int fa1 = 20;
           return fa1;
           }

0x08048412 int f(int fx, int fy){
           int fa = 10, fb = 12;
0x08048439 f1(fx, fy, fa);
           return fb;
           }

0x08048446 int g(int gx, int gy){
           return gx + gy;
           }

0x0804845d int main(){
           int a = 3, b = 5, c = 7;
           f(a,b);
           g(b,c);
           return 0;
           }
  
```

EBP

0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

```

0x080483f6 int f1(int fx1, int fy1, int fz1){
           int fa1 = 20;
           return fa1;
           }

0x08048412 int f(int fx, int fy){
           int fa = 10, fb = 12;
0x08048439 f1(fx, fy, fa);
           return fb;
           }

0x08048446 int g(int gx, int gy){
           return gx + gy;
           }

0x0804845d int main(){
           int a = 3, b = 5, c = 7;
0x08048488 f(a,b);
0x08048496 g(b,c);
           return 0;
           }

```

**Resets the previous EBP**

EBP

0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

```

0x080483f6 int f1(int fx1, int fy1, int fz1){
           int fa1 = 20;
           return fa1;
           }

0x08048412 int f(int fx, int fy){
           int fa = 10, fb = 12;
0x08048439 f1(fx, fy, fa);
           return fb;
           }

0x08048446 int g(int gx, int gy){
           return gx + gy;
           }

0x0804845d int main(){
           int a = 3, b = 5, c = 7;
           f(a,b);
           g(b,c);
           return 0;
           }

```

**Resets the previous EBP**

EBP

0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

# Program Execution

```

0x080483f6 int f1(int fx1, int fy1, int fz1){
           int fa1 = 20;
           return fa1;
           }

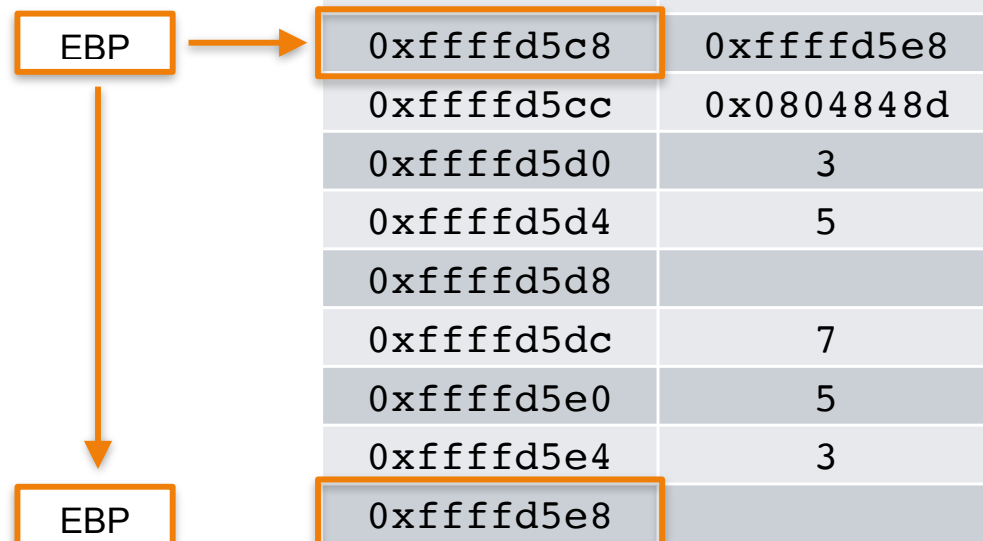
0x08048412 int f(int fx, int fy){
           int fa = 10, fb = 12;
0x08048439 f1(fx, fy, fa);
           return fb;
           }

0x08048446 int g(int gx, int gy){
           return gx + gy;
           }

0x0804845d int main(){
           int a = 3, b = 5, c = 7;
           f(a,b);
           g(b,c);
           return 0;
           }

```

**Resets the previous EBP**



# Program Execution

0x080483f6	<code>int f1(int fx1, int fy1, int fz1){</code>
	<code>int fa1 = 20;</code>
	<code>return fa1;</code>
	<code>}</code>
0x08048412	<code>int f(int fx, int fy){</code>
	<code>int fa = 10, fb = 12;</code>
0x08048439	<code>f1(fx, fy, fa);</code>
	<code>return fb;</code>
	<code>}</code>
0x08048446	<code>int g(int gx, int gy){</code>
	<code>return gx + gy;</code>
	<code>}</code>
0x0804845d	<code>int main(){</code>
	<code>int a = 3, b = 5, c = 7;</code>
0x08048488	<code>f(a,b);</code>
0x08048496	<code>g(b,c);</code>
	<code>return 0;</code>
	<code>}</code>

**Resets the previous EBP**

0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

EBP



# Program Execution

**Continues where it  
stoped in main**

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

EBP

# Program Execution

**Continues where it  
stoped in main**

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

EBP

# Program Execution

And the frame of **f**  
Becomes unused

0x080483f6	int f1(int fx1, int fy1, int fz1){
	int fa1 = 20;
	return fa1;
	}
0x08048412	int f(int fx, int fy){
	int fa = 10, fb = 12;
0x08048439	f1(fx, fy, fa);
	return fb;
	}
0x08048446	int g(int gx, int gy){
	return gx + gy;
	}
0x0804845d	int main(){
	int a = 3, b = 5, c = 7;
0x08048488	f(a,b);
0x08048496	g(b,c);
	return 0;
	}

0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

EBP



# Program Execution

And the frame of **f**  
Becomes unused

```
0x080483f6 int f1(int fx1, int fy1, int fz1){
            int fa1 = 20;
            return fa1;
        }
```

```
0x08048412 int f(int fx, int fy){
            int fa = 10, fb = 12;
0x08048439 f1(fx, fy, fa);
            return fb;
        }
```

```
0x08048446 int g(int gx, int gy){
            return gx + gy;
        }
```

```
0x0804845d int main(){
            int a = 3, b = 5, c = 7;
0x08048488 f(a,b);
0x08048496 g(b,c);
            return 0;
        }
```

0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

EBP

0xffffd5e8

# Program Execution

```

0x080483f6 int f1(int fx1, int fy1, int fz1){
           int fa1 = 20;
           return fa1;
           }

```

```

0x08048412 int f(int fx, int fy){
           int fa = 10, fb = 12;
0x08048439 f1(fx, fy, fa);
           return fb;
           }

```

```

0x08048446 int g(int gx, int gy){
           return gx + gy;
           }

```

```

0x0804845d int main(){
           int a = 3, b = 5, c = 7;
0x08048488 f(a,b);
0x08048496 g(b,c);
           return 0;
           }

```

Repeat for g

0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

EBP

# Program Execution

```
0x080483f6 int f1(int fx1, int fy1, int fz1){
            int fa1 = 20;
            return fa1;
        }
```

```
0x08048412 int f(int fx, int fy){
            int fa = 10, fb = 12;
0x08048439 f1(fx, fy, fa);
            return fb;
        }
```

```
0x08048446 int g(int gx, int gy){
            return gx + gy;
        }
```

```
0x0804845d int main(){
            int a = 3, b = 5, c = 7;
0x08048488 f(a,b);
0x08048496 g(b,c);
            return 0;
        }
```

Repeat for g

0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

EBP