#### x86\_32bit Program Execution

Segurança em Software Pedro Adão, Ana Matos

(and Miguel Correia)



```
int f1(int fx1, int fy1, int fz1){
0x080483f6
                int fa1 = 20:
                return fa1;
            int f(int fx, int fy){
0 \times 08048412
                int fa = 10, fb = 12;
                f1(fx, fy, fa);
0x08048439
                return fb;
            int q(int gx, int gy){
0 \times 08048446
                return gx + gy;
            int main(){
0x0804845d
                int a = 3, b = 5, c = 7;
                f(a,b);
0 \times 08048488
                g(b,c);
0x08048496
                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
                           eax, DWORD PTR [ebp-0x4]
 0x0804840d <+23>: mov
 0x08048410 <+26>: leave
 0 \times 08048411 < +27>: ret
Dump of assembler code for function f:
 0x08048412 <+0>: push
                           ebp
                           ebp,esp
 0x08048413 <+1>: mov
 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>
 0 \times 0804843e < +44>: add
                           esp,0xc
                           eax.DWORD PTR [ebp-0x8]
 0x08048441 <+47>: mov
 0x08048444 <+50>: leave
 0 \times 08048445 < +51>: ret
```

```
int f1(int fx1, int fy1, int fz1){
0x080483f6
                int fa1 = 20:
                return fa1;
           int f(int fx, int fy){
0x08048412
                int fa = 10, fb = 12;
                f1(fx, fy, fa);
0x08048439
                return fb;
           int q(int gx, int gy){
0x08048446
                return gx + gy;
           int main(){
0x0804845d
                int a = 3, b = 5, c = 7;
                f(a,b);
0 \times 08048488
                q(b,c);
0x08048496
                return 0;
```

```
Dump of assembler code for function f1:
 0x080483f6 <+0>: push
                           ebp
 0 \times 080483f7 < +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
                           eax, DWORD PTR [ebp-0x4]
 0x0804840d <+23>: mov
 0x08048410 <+26>: leave
 0 \times 08048411 < +27>: ret
Dump of assembler code for function f:
                           ebp
 0x08048412 <+0>: push
 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>
                           esp,0xc
 0x0804843e <+44>: add
                           eax.DWORD PTR [ebp-0x8]
 0x08048441 <+47>: mov
 0x08048444 <+50>: leave
 0 \times 08048445 < +51>: ret
```

```
int f1(int fx1, int fy1, int fz1){
0x080483f6
                int fa1 = 20;
                return fa1;
            int f(int fx, int fy){
0 \times 08048412
                int fa = 10, fb = 12;
                f1(fx, fy, fa);
0x08048439
                return fb;
            int g(int gx, int gy){
0x08048446
                return qx + qy;
            int main(){
0x0804845d
                int a = 3, b = 5, c = 7;
                f(a,b);
0 \times 08048488
                g(b,c);
0x08048496
                return 0;
```

```
Dump of assembler code for function g:
  0x08048446 <+0>: push
                            ebp
 0 \times 08048447 < +1>: mov
                            ebp,esp
                            0x80484a5 < x86.get pc thunk.ax>
 0x08048449 <+3>: call
 0x0804844e <+8>: add
                            eax.0x1bb2
  0x08048453 <+13>: mov
                            edx, DWORD PTR [ebp+0x8]
                            eax, DWORD PTR [ebp+0xc]
 0x08048456 <+16>: mov
  0 \times 08048459 < +19>: add
                            eax,edx
 0x0804845b <+21>: pop
                            ebp
 0 \times 0804845c < +22>: ret
Dump of assembler code for function main:
 0x0804845d <+0>: push
                            ebp
  0x0804845e <+1>: mov
                            ebp,esp
 0x08048460 <+3>: sub
                            esp.0x10
                            0x80484a5 <__x86.get_pc_thunk.ax>
  0x08048463 <+6>: call
 0 \times 08048468 < +11>: add
                            eax,0x1b98
 0x0804846d <+16>: mov
                            DWORD PTR [ebp-0x4], 0x3
                            DWORD PTR [ebp-0x8], 0x5
  0 \times 08048474 < +23 > : mov
  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>
                            esp,0x8
  0x0804848d <+48>: add
 0x08048490 <+51>: push
                            DWORD PTR [ebp-0xc]
 0x08048493 <+54>: push
                            DWORD PTR [ebp-0x8]
  0x08048496 <+57>: call
                            0x8048446 <q>
 0x0804849b <+62>: add
                            esp,0x8
  0 \times 0804849e < +65 > : mov
                            eax,0x0
  0x080484a3 <+70>: leave
  0 \times 080484a4 < +71 > : ret
```

```
int f1(int fx1, int fy1, int fz1){
0x080483f6
                int fa1 = 20;
                return fa1;
            int f(int fx, int fy){
0 \times 08048412
                int fa = 10, fb = 12;
                f1(fx, fy, fa);
0x08048439
                return fb;
            int g(int gx, int gy){
0x08048446
                return qx + qy;
            int main(){
0x0804845d
                int a = 3, b = 5, c = 7;
                f(a,b);
0 \times 08048488
                g(b,c);
0x08048496
                return 0;
```

```
Dump of assembler code for function g:
 0x08048446 <+0>:
                    push
                            ebp
  0 \times 08048447 < +1>: mov
                            ebp, esp
  0x08048449 <+3>: call
                            0x80484a5 < x86.get pc thunk.ax>
 0x0804844e <+8>: add
                            eax.0x1bb2
                            edx, DWORD PTR [ebp+0x8]
  0x08048453 <+13>: mov
                            eax, DWORD PTR [ebp+0xc]
 0x08048456 <+16>: mov
  0 \times 08048459 < +19>: add
                            eax,edx
 0x0804845b <+21>: pop
                            ebp
 0 \times 0804845c < +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>
 0 \times 08048468 < +11>: add
                            eax,0x1b98
                            DWORD PTR [ebp-0x4], 0x3
 0x0804846d <+16>: mov
                            DWORD PTR [ebp-0x8], 0x5
  0 \times 08048474 < +23 > : mov
  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 <q>
  0 \times 0804849b < +62>: add
                            esp,0x8
  0 \times 0804849e < +65 > : mov
                            eax,0x0
  0x080484a3 <+70>: leave
  0 \times 080484a4 < +71 > : ret
```

#### Stack Layout

0x00000000

Low addresses are on the top (stack goes up)

local vars 2nd function saved EBP return address (aka saved EIP) parameters 2nd function local vars 1st function saved EBP return address (aka saved EIP) parameters 1st function local vars function main saved EBP return address (aka saved EIP) args function main

Stack frame 1st function

Stack frame function main

0xfffffff

```
int f1(int fx1, int fy1, int fz1){
0x080483f6
                int fa1 = 20;
                return fa1;
           int f(int fx, int fy){
0x08048412
                int fa = 10, fb = 12;
                f1(fx, fy, fa);
0x08048439
                return fb;
           int q(int qx, int qy){
0x08048446
                return gx + gy;
           int main(){
0x0804845d
                int a = 3, b = 5, c = 7;
                f(a,b);
0 \times 08048488
                g(b,c);
0x08048496
                return 0;
```

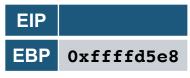
We start with main

```
int f1(int fx1, int fy1, int fz1){
0x080483f6
               int fa1 = 20;
               return fa1;
           int f(int fx, int fy){
0x08048412
               int fa = 10, fb = 12;
               f1(fx, fy, fa);
0x08048439
               return fb;
           int g(int gx, int gy){
0x08048446
               return gx + gy;
           int main(){
0x0804845d
               int a = 3, b = 5, c = 7;
               f(a,b);
0 \times 08048488
                                                                 We start with main
               g(b,c);
0x08048496
               return 0;
                                                               0xffffd5e8
                                               EBP
```

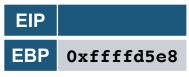


```
int f1(int fx1, int fy1, int fz1){
0x080483f6
               int fa1 = 20;
               return fa1;
           int f(int fx, int fy){
0x08048412
               int fa = 10, fb = 12;
               f1(fx, fy, fa);
0x08048439
               return fb;
           int q(int qx, int qy){
0x08048446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

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



```
int f1(int fx1, int fy1, int fz1){
0x080483f6
               int fa1 = 20;
               return fa1;
           int f(int fx, int fy){
0x08048412
               int fa = 10, fb = 12;
               f1(fx, fy, fa);
0x08048439
               return fb;
           int g(int gx, int gy){
0x08048446
               return qx + qy;
                                                                Next we push the
                                                             local variables of main
                                                                     (in order)
           int main(){
0x0804845d
               int a = 3, b = 5, c = 7;
               f(a,b);
0x08048488
               g(b,c);
0x08048496
               return 0;
                                                            0xffffd5e4
                                                                                   3
                                             EBP
                                                            0xffffd5e8
```



```
int f1(int fx1, int fy1, int fz1){
0x080483f6
               int fa1 = 20;
               return fa1;
           int f(int fx, int fy){
0x08048412
               int fa = 10, fb = 12;
               f1(fx, fy, fa);
0x08048439
               return fb;
           int g(int gx, int gy){
0x08048446
               return qx + qy;
                                                                Next we push the
                                                            local variables of main
                                                                     (in order)
           int main(){
0x0804845d
               int a = 3, b = 5, c = 7;
               f(a,b);
0x08048488
               g(b,c);
0x08048496
                                                            0xffffd5e0
               return 0;
                                                            0xffffd5e4
                                             EBP
                                                            0xffffd5e8
```



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

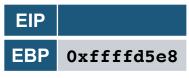
Next we push the local variables of main (in order)

0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	



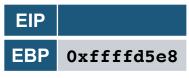
```
int f1(int fx1, int fy1, int fz1){
0x080483f6
               int fa1 = 20;
               return fa1;
           int f(int fx, int fy){
0x08048412
               int fa = 10, fb = 12;
               f1(fx, fy, fa);
0x08048439
               return fb;
           int g(int gx, int gy){
0x08048446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

0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	



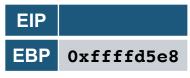
```
int f1(int fx1, int fy1, int fz1){
0x080483f6
               int fa1 = 20;
               return fa1;
           int f(int fx, int fy){
0x08048412
               int fa = 10, fb = 12;
               f1(fx, fy, fa);
0x08048439
               return fb;
           int g(int gx, int gy){
0x08048446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

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



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

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



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

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

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

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

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

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

```
int f1(int fx1, int fy1, int fz1){
0x080483f6
                int fa1 = 20;
                return fa1;
           int f(int fx, int fy){
0x08048412
                int fa = 10, fb = 12;
                f1(fx, fy, fa);
0x08048439
                return fb;
           int g(int gx, int gy){
0x08048446
                return gx + gy;
           int main(){
0x0804845d
                int a = 3, b = 5, c = 7;
                f(a,b);
0 \times 08048488
                g(b,c);
0x08048496
                return 0;
                                                EBP
```

When entering f push the address of EBP of main

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

```
int f1(int fx1, int fy1, int fz1){
0x080483f6
                int fa1 = 20;
                return fa1;
           int f(int fx, int fy){
0x08048412
                int fa = 10, fb = 12;
                f1(fx, fy, fa);
0x08048439
                return fb;
           int g(int gx, int gy){
0x08048446
                return gx + gy;
           int main(){
0x0804845d
                int a = 3, b = 5, c = 7;
                f(a,b);
0 \times 08048488
                g(b,c);
0x08048496
                return 0;
                                                EBP
```

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	

And set the

new EBP of f

0x0804848d

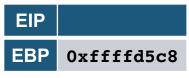
5

```
int f1(int fx1, int fy1, int fz1){
0x080483f6
               int fa1 = 20;
               return fa1;
           int f(int fx, int fy){
0x08048412
               int fa = 10, fb = 12;
               f1(fx, fy, fa);
0x08048439
               return fb;
           int g(int gx, int gy){
0x08048446
               return qx + qy;
                                                             0xffffd5cc
                                                             0xffffd5d0
           int main(){
0x0804845d
                                                             0xffffd5d4
               int a = 3, b = 5, c = 7;
                                                             0xffffd5d8
               f(a,b);
0 \times 08048488
                                                             0xffffd5dc
               g(b,c);
0x08048496
                                                             0xffffd5e0
               return 0;
                                                             0xffffd5e4
                                              EBP
                                                             0xffffd5e8
```

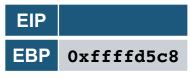
```
int f1(int fx1, int fy1, int fz1){
0x080483f6
               int fa1 = 20;
               return fa1;
                                                                   And set the
          int f(int fx, int fy){
0x08048412
                                                                  new EBP of f
               int fa = 10, fb = 12;
               f1(fx, fy, fa);
0x08048439
               return fb;
          int g(int gx, int gy){
0x08048446
                                             EBP
                                                            0xffffd5c8
                                                                            0xffffd5e8
               return gx + gy;
                                                            0xffffd5cc
                                                                            0x0804848d
                                                            0xffffd5d0
          int main(){
0x0804845d
                                                            0xffffd5d4
               int a = 3, b = 5, c = 7;
                                                            0xffffd5d8
               f(a,b);
0 \times 08048488
                                                            0xffffd5dc
               g(b,c);
0x08048496
                                                            0xffffd5e0
                                                                                  5
               return 0;
                                                            0xffffd5e4
                                             EBP
                                                            0xffffd5e8
```

EIP 0x08048412
EBP 0xffffd5c8

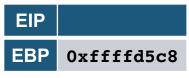
```
int f1(int fx1, int fy1, int fz1){
0x080483f6
               int fa1 = 20;
               return fa1;
                                                                   And set the
          int f(int fx, int fy){
0x08048412
                                                                  new EBP of f
               int fa = 10, fb = 12;
               f1(fx, fy, fa);
0x08048439
               return fb;
          int g(int gx, int gy){
0x08048446
                                                            0xffffd5c8
                                                                            0xffffd5e8
                                             EBP
               return gx + gy;
                                                            0xffffd5cc
                                                                            0x0804848d
                                                            0xffffd5d0
          int main(){
0x0804845d
                                                            0xffffd5d4
               int a = 3, b = 5, c = 7;
                                                            0xffffd5d8
               f(a,b);
0 \times 08048488
                                                            0xffffd5dc
               g(b,c);
0x08048496
                                                            0xffffd5e0
                                                                                  5
               return 0;
                                                            0xffffd5e4
                                                            0xffffd5e8
```



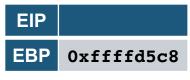
```
int f1(int fx1, int fy1, int fz1){
0x080483f6
               int fa1 = 20;
               return fa1;
                                                               Next we push the
                                                              local variables of f
          int f(int fx, int fy){
0x08048412
                                                                    (in order)
               int fa = 10, fb = 12;
               f1(fx, fy, fa);
0x08048439
               return fb;
          int g(int gx, int gy){
0x08048446
                                                            0xffffd5c8
                                                                            0xffffd5e8
                                             EBP
               return qx + qy;
                                                            0xffffd5cc
                                                                            0x0804848d
                                                            0xffffd5d0
          int main(){
0x0804845d
                                                            0xffffd5d4
               int a = 3, b = 5, c = 7;
                                                            0xffffd5d8
               f(a,b);
0 \times 08048488
                                                            0xffffd5dc
               g(b,c);
0x08048496
                                                            0xffffd5e0
                                                                                  5
               return 0;
                                                            0xffffd5e4
                                                            0xffffd5e8
```



```
int f1(int fx1, int fy1, int fz1){
0x080483f6
              int fa1 = 20;
              return fa1;
                                                               Next we push the
                                                              local variables of f
          int f(int fx, int fy){
0x08048412
                                                                    (in order)
              int fa = 10, fb = 12;
              f1(fx, fy, fa);
0x08048439
              return fb;
                                                           0xffffd5c4
                                                                                10
          int g(int gx, int gy){
0x08048446
                                             EBP
                                                           0xffffd5c8
                                                                            0xffffd5e8
              return qx + qy;
                                                           0xffffd5cc
                                                                            0x0804848d
                                                           0xffffd5d0
          int main(){
0x0804845d
                                                           0xffffd5d4
              int a = 3, b = 5, c = 7;
                                                           0xffffd5d8
              f(a,b);
0 \times 08048488
                                                           0xffffd5dc
              g(b,c);
0x08048496
                                                           0xffffd5e0
                                                                                 5
              return 0;
                                                           0xffffd5e4
                                                           0xffffd5e8
```



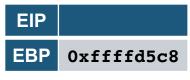
```
int f1(int fx1, int fy1, int fz1){
0x080483f6
              int fa1 = 20;
              return fa1;
                                                               Next we push the
                                                              local variables of f
          int f(int fx, int fy){
0x08048412
                                                                    (in order)
              int fa = 10, fb = 12;
              f1(fx, fy, fa);
0x08048439
              return fb;
                                                           0xffffd5c0
                                                                                12
                                                           0xffffd5c4
                                                                                10
          int g(int gx, int gy){
0x08048446
                                            EBP
                                                           0xffffd5c8
                                                                            0xffffd5e8
              return qx + qy;
                                                           0xffffd5cc
                                                                            0x0804848d
                                                           0xffffd5d0
          int main(){
0x0804845d
                                                           0xffffd5d4
              int a = 3, b = 5, c = 7;
                                                           0xffffd5d8
              f(a,b);
0 \times 08048488
                                                           0xffffd5dc
              g(b,c);
0x08048496
                                                           0xffffd5e0
                                                                                 5
              return 0;
                                                           0xffffd5e4
                                                           0xffffd5e8
```



And call function f1
pushing the parameters of f1
(in reverse order)

```
int f1(int fx1, int fy1, int fz1){
0x080483f6
                int fa1 = 20;
                return fa1;
           int f(int fx, int fy){
0x08048412
                int fa = 10, fb = 12;
                f1(fx, fy, fa);
0x08048439
                return fb;
           int q(int qx, int qy){
0x08048446
                                                EBP
                return gx + gy;
           int main(){
0x0804845d
                int a = 3, b = 5, c = 7;
                f(a,b);
0 \times 08048488
                g(b,c);
0x08048496
                return 0;
```

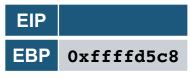
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	



And call function £1 pushing the parameters of £1 (in reverse order)

```
int f1(int fx1, int fy1, int fz1){
0x080483f6
                int fa1 = 20;
                return fa1;
           int f(int fx, int fy){
0x08048412
                int fa = 10, fb = 12;
                f1(fx, fy, fa);
0x08048439
                return fb;
           int g(int gx, int gy){
0x08048446
                                                EBP
                return gx + gy;
           int main(){
0x0804845d
                int a = 3, b = 5, c = 7;
                f(a,b);
0 \times 08048488
                g(b,c);
0x08048496
                return 0;
```

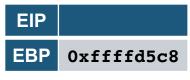
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	



And call function £1 pushing the parameters of £1 (in reverse order)

```
int f1(int fx1, int fy1, int fz1){
0x080483f6
                int fa1 = 20;
                return fa1;
           int f(int fx, int fy){
0x08048412
                int fa = 10, fb = 12;
                f1(fx, fy, fa);
0x08048439
                return fb;
           int g(int gx, int gy){
0x08048446
                                                EBP
                return gx + gy;
           int main(){
0x0804845d
                int a = 3, b = 5, c = 7;
                f(a,b);
0 \times 08048488
                g(b,c);
0x08048496
                return 0;
```

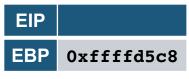
0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	



And call function £1 pushing the parameters of £1 (in reverse order)

```
int f1(int fx1, int fy1, int fz1){
0x080483f6
                int fa1 = 20;
                return fa1;
           int f(int fx, int fy){
0x08048412
                int fa = 10, fb = 12;
                f1(fx, fy, fa);
0x08048439
                return fb;
           int g(int gx, int gy){
0x08048446
                                                EBP
                return gx + gy;
           int main(){
0x0804845d
                int a = 3, b = 5, c = 7;
                f(a,b);
0 \times 08048488
                g(b,c);
0x08048496
                return 0;
```

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	



And call function f1
pushing the parameters of f1
(in reverse order)

```
int f1(int fx1, int fy1, int fz1){
0x080483f6
                int fa1 = 20;
                return fa1;
           int f(int fx, int fy){
0x08048412
                int fa = 10, fb = 12;
                f1(fx, fy, fa);
0x08048439
                return fb;
           int g(int gx, int gy){
0x08048446
                                                EBP
                return gx + gy;
           int main(){
0x0804845d
                int a = 3, b = 5, c = 7;
                f(a,b);
0 \times 08048488
                g(b,c);
0x08048496
                return 0;
```

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	

And the address of f where to continue when f1 finishes

```
int f1(int fx1, int fy1, int fz1){
0x080483f6
                int fa1 = 20;
                return fa1;
           int f(int fx, int fy){
0x08048412
                int fa = 10, fb = 12;
                f1(fx, fy, fa);
0x08048439
                return fb;
           int q(int qx, int qy){
0x08048446
                                                EBP
                return gx + gy;
           int main(){
0x0804845d
                int a = 3, b = 5, c = 7;
                f(a,b);
0 \times 08048488
                g(b,c);
0x08048496
                return 0;
```

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	

And the address of f where to continue when f1 finishes

```
int f1(int fx1, int fy1, int fz1){
0x080483f6
                int fa1 = 20;
                return fa1;
           int f(int fx, int fy){
0x08048412
                int fa = 10, fb = 12;
                f1(fx, fy, fa);
0x08048439
                return fb;
           int g(int gx, int gy){
0x08048446
                                                EBP
                return gx + gy;
           int main(){
0x0804845d
                int a = 3, b = 5, c = 7;
                f(a,b);
0 \times 08048488
                g(b,c);
0x08048496
                return 0;
```

0x0804843e
3
5
10
12
10
0xffffd5e8
0x0804848d
3
5
7
7 5
· · · · · · · · · · · · · · · · · · ·

When entering f1 push the address of EBP of f

```
0x080483f6
           int f1(int fx1, int fy1, int fz1){
                int fa1 = 20;
                return fa1;
           int f(int fx, int fy){
0x08048412
                int fa = 10, fb = 12;
                f1(fx, fy, fa);
0x08048439
                return fb;
           int q(int qx, int qy){
0x08048446
                                                EBP
                return gx + gy;
           int main(){
0x0804845d
                int a = 3, b = 5, c = 7;
                f(a,b);
0 \times 08048488
                g(b,c);
0x08048496
                return 0;
```

0xffffd5ac	0x0804843e
0xffffd5b0	3
0xffffd5b4	5
0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
UNITITIES	0X0004040U
0xffffd5d0	3
0xffffd5d0	3
0xffffd5d0 0xffffd5d4	3
0xffffd5d0 0xffffd5d4 0xffffd5d8	3 5
0xffffd5d0 0xffffd5d4 0xffffd5d8 0xffffd5dc	3 5 7
0xffffd5d0 0xffffd5d4 0xffffd5d8 0xffffd5dc 0xffffd5e0	3 5 7 5

When entering f1 push the address of EBP of f

```
0x080483f6
           int f1(int fx1, int fy1, int fz1){
                int fa1 = 20;
                return fa1;
           int f(int fx, int fy){
0x08048412
                int fa = 10, fb = 12;
                f1(fx, fy, fa);
0x08048439
                return fb;
           int g(int gx, int gy){
0x08048446
                                                EBP
                return gx + gy;
           int main(){
0x0804845d
                int a = 3, b = 5, c = 7;
                f(a,b);
0 \times 08048488
                g(b,c);
0x08048496
                return 0;
```

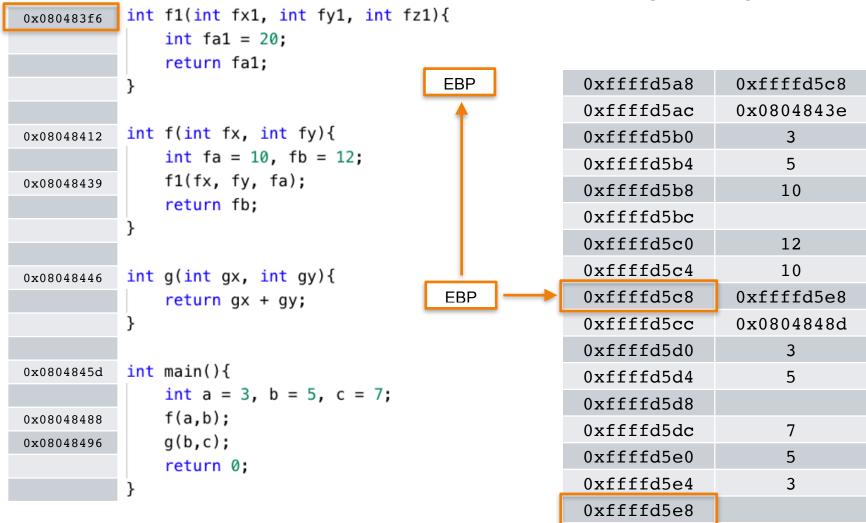
0xffffd5a8	0xffffd5c8
0xffffd5ac	0x0804843e
0xffffd5b0	3
0xffffd5b4	5
0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

And set the new EBP of £1

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

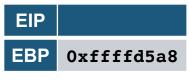
0xffffd5ac	0x0804843e
0xffffd5b0	3
0xffffd5b4	5
0xffffd5b8	10
0xffffd5bc	
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	

And set the new EBP of f1



And set the new EBP of f1

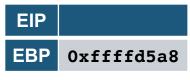
```
0x080483f6
          int f1(int fx1, int fy1, int fz1){
              int fa1 = 20;
              return fa1;
                                                           0xffffd5a8
                                                                           0xffffd5c8
                                            EBP
                                                           0xffffd5ac
                                                                           0x0804843e
          int f(int fx, int fy){
                                                           0xffffd5b0
0x08048412
              int fa = 10, fb = 12;
                                                           0xffffd5b4
              f1(fx, fy, fa);
0x08048439
                                                           0xffffd5b8
                                                                                10
              return fb;
                                                           0xffffd5bc
                                                           0xffffd5c0
                                                                                12
                                                           0xffffd5c4
                                                                                10
          int g(int gx, int gy){
0x08048446
                                                                           0xffffd5e8
                                                           0xffffd5c8
              return qx + qy;
                                                           0xffffd5cc
                                                                           0x0804848d
                                                           0xffffd5d0
          int main(){
0x0804845d
                                                           0xffffd5d4
              int a = 3, b = 5, c = 7;
                                                           0xffffd5d8
              f(a,b);
0 \times 08048488
                                                           0xffffd5dc
              g(b,c);
0x08048496
                                                           0xffffd5e0
                                                                                 5
              return 0;
                                                           0xffffd5e4
                                                           0xffffd5e8
```



# Program Exect Next we push the

local variables of f1 (in order)

0x080483f6	int	f1(int fx1, int fy1, int f	z1){	•	,
		<pre>int fa1 = 20;</pre>			
	}	return fa1;	EBP -	0xffffd5a8	0xffffd5c8
				0xffffd5ac	0x0804843e
0x08048412	int	f(int fx, int fy){		0xffffd5b0	3
		int fa = 10, fb = 12;		0xffffd5b4	5
0x08048439		f1(fx, fy, fa);		0xffffd5b8	10
	] }	return fb;		0xffffd5bc	
	,			0xffffd5c0	12
0x08048446	int	g(int gx, int gy){		0xffffd5c4	10
		return gx + gy;		0xffffd5c8	0xffffd5e8
	}			0xffffd5cc	0x0804848d
				0xffffd5d0	3
0x0804845d	int	main(){		0xffffd5d4	5
		int $a = 3$ , $b = 5$ , $c = 7$ ;		0xffffd5d8	
0x08048488		f(a,b);		0xffffd5dc	7
0x08048496		g(b,c); return 0;		0xffffd5e0	5
	}	recurr 0,		0xffffd5e4	3
	•			0xffffd5e8	
					·

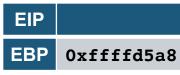


## Program Exect Next we push the local variables of f

local variables of £1 (in order)

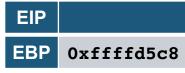
```
int f1(int fx1, int fy1, int fz1){
0x080483f6
               int fa1 = 20;
               return fa1;
                                               EBP
           int f(int fx, int fy){
0x08048412
               int fa = 10, fb = 12;
               f1(fx, fy, fa);
0x08048439
               return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

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	



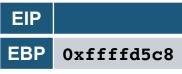
## Program Execument returns

```
int f1(int fx1, int fy1, int fz1){
0x080483f6
                                                           0xffffd5a0
              int fa1 = 20;
                                                           0xffffd5a4
                                                                               20
              return fa1;
                                            EBP
                                                           0xffffd5a8
                                                                           0xffffd5c8
                                                           0xffffd5ac
                                                                           0x0804843e
          int f(int fx, int fy){
                                                           0xffffd5b0
                                                                                3
0x08048412
              int fa = 10, fb = 12;
                                                           0xffffd5b4
              f1(fx, fy, fa);
0x08048439
                                                           0xffffd5b8
                                                                               10
              return fb;
                                                           0xffffd5bc
                                                           0xffffd5c0
                                                                               12
                                                           0xffffd5c4
                                                                               10
          int g(int gx, int gy){
0x08048446
                                                           0xffffd5c8
                                                                           0xffffd5e8
              return qx + qy;
                                                           0xffffd5cc
                                                                           0x0804848d
                                                           0xffffd5d0
          int main(){
0x0804845d
                                                           0xffffd5d4
              int a = 3, b = 5, c = 7;
                                                           0xffffd5d8
              f(a,b);
0 \times 08048488
                                                           0xffffd5dc
              g(b,c);
0x08048496
                                                           0xffffd5e0
                                                                                5
              return 0;
                                                           0xffffd5e4
                                                           0xffffd5e8
```

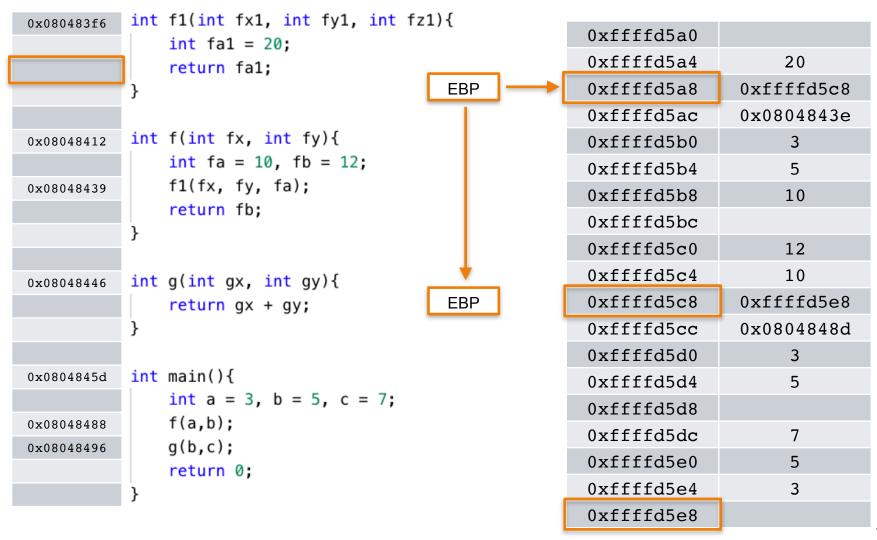


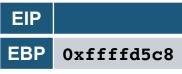
#### Program Exe(Resets the previous EBP

```
int f1(int fx1, int fy1, int fz1){
0x080483f6
                                                           0xffffd5a0
              int fa1 = 20;
                                                           0xffffd5a4
                                                                               20
              return fa1;
                                            EBP
                                                           0xffffd5a8
                                                                           0xffffd5c8
                                                           0xffffd5ac
                                                                           0x0804843e
          int f(int fx, int fy){
                                                           0xffffd5b0
                                                                                3
0x08048412
              int fa = 10, fb = 12;
                                                           0xffffd5b4
              f1(fx, fy, fa);
0x08048439
                                                           0xffffd5b8
                                                                               10
              return fb;
                                                           0xffffd5bc
                                                           0xffffd5c0
                                                                               12
                                                           0xffffd5c4
                                                                               10
          int g(int gx, int gy){
0x08048446
                                                           0xffffd5c8
                                                                           0xffffd5e8
              return qx + qy;
                                                           0xffffd5cc
                                                                           0x0804848d
                                                           0xffffd5d0
          int main(){
0x0804845d
                                                           0xffffd5d4
              int a = 3, b = 5, c = 7;
                                                           0xffffd5d8
              f(a,b);
0 \times 08048488
                                                           0xffffd5dc
              g(b,c);
0x08048496
                                                           0xffffd5e0
                                                                                5
              return 0;
                                                           0xffffd5e4
                                                                                3
                                                           0xffffd5e8
```



#### Program Exe(Resets the previous EBP





#### Program Exe(Resets the previous EBP

```
int f1(int fx1, int fy1, int fz1){
0x080483f6
                                                           0xffffd5a0
              int fa1 = 20;
                                                           0xffffd5a4
                                                                               20
              return fa1;
                                                                           0xffffd5c8
                                                           0xffffd5a8
                                                           0xffffd5ac
                                                                           0x0804843e
          int f(int fx, int fy){
                                                           0xffffd5b0
                                                                                3
0x08048412
              int fa = 10, fb = 12;
                                                           0xffffd5b4
              f1(fx, fy, fa);
0x08048439
                                                           0xffffd5b8
                                                                               10
              return fb;
                                                           0xffffd5bc
                                                           0xffffd5c0
                                                                               12
                                                           0xffffd5c4
                                                                               10
          int g(int gx, int gy){
0x08048446
                                            EBP
                                                           0xffffd5c8
                                                                           0xffffd5e8
              return gx + gy;
                                                           0xffffd5cc
                                                                           0x0804848d
                                                           0xffffd5d0
          int main(){
0x0804845d
                                                           0xffffd5d4
              int a = 3, b = 5, c = 7;
                                                           0xffffd5d8
              f(a,b);
0 \times 08048488
                                                           0xffffd5dc
              g(b,c);
0x08048496
                                                           0xffffd5e0
                                                                                5
              return 0;
                                                           0xffffd5e4
                                                                                3
                                                           0xffffd5e8
```

# Program Exect continues where it stoped in f

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

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 Exectand the frame of £1 Becomes unused

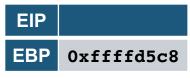
```
int f1(int fx1, int fy1, int fz1){
0x080483f6
               int fa1 = 20;
               return fa1;
           int f(int fx, int fy){
0x08048412
               int fa = 10, fb = 12;
               f1(fx, fy, fa);
0x08048439
               return fb;
           int g(int gx, int gy){
0x08048446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

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

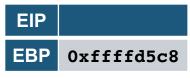


## Program Exect And the frame of £1 Becomes unused

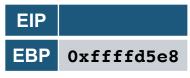
```
int f1(int fx1, int fy1, int fz1){
0x080483f6
               int fa1 = 20;
               return fa1;
           int f(int fx, int fy){
0x08048412
               int fa = 10, fb = 12;
               f1(fx, fy, fa);
0x08048439
               return fb;
                                                            0xffffd5bc
                                                            0xffffd5c0
                                                                                  12
                                                            0xffffd5c4
                                                                                  10
           int g(int gx, int gy){
0x08048446
                                                            0xffffd5c8
                                                                             0xffffd5e8
                                             EBP
               return qx + qy;
                                                            0xffffd5cc
                                                                             0x0804848d
                                                            0xffffd5d0
           int main(){
0x0804845d
                                                            0xffffd5d4
               int a = 3, b = 5, c = 7;
                                                            0xffffd5d8
               f(a,b);
0 \times 08048488
                                                            0xffffd5dc
               g(b,c);
0x08048496
                                                            0xffffd5e0
                                                                                  5
               return 0;
                                                            0xffffd5e4
                                                                                  3
                                                            0xffffd5e8
```



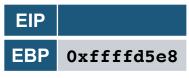
```
int f1(int fx1, int fy1, int fz1){
0x080483f6
              int fa1 = 20;
              return fa1;
          int f(int fx, int fy){
0x08048412
                                                                When f returns
              int fa = 10, fb = 12;
              f1(fx, fy, fa);
0x08048439
              return fb;
                                                           0xffffd5bc
                                                           0xffffd5c0
                                                                                 12
                                                           0xffffd5c4
                                                                                10
          int g(int gx, int gy){
0x08048446
                                                           0xffffd5c8
                                                                            0xffffd5e8
                                            EBP
              return gx + gy;
                                                           0xffffd5cc
                                                                            0x0804848d
                                                           0xffffd5d0
          int main(){
0x0804845d
                                                           0xffffd5d4
              int a = 3, b = 5, c = 7;
                                                           0xffffd5d8
              f(a,b);
0 \times 08048488
                                                           0xffffd5dc
              g(b,c);
0x08048496
                                                           0xffffd5e0
                                                                                 5
              return 0;
                                                           0xffffd5e4
                                                           0xffffd5e8
```



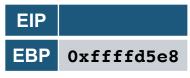
```
int f1(int fx1, int fy1, int fz1){
0x080483f6
               int fa1 = 20;
               return fa1;
          int f(int fx, int fy){
0x08048412
                                                                When f returns
               int fa = 10, fb = 12;
               f1(fx, fy, fa);
0x08048439
               return fb;
                                                            0xffffd5c0
                                                                                 12
                                                            0xffffd5c4
                                                                                 10
          int g(int gx, int gy){
0x08048446
                                                            0xffffd5c8
                                                                            0xffffd5e8
                                            EBP
               return gx + gy;
                                                            0xffffd5cc
                                                                            0x0804848d
                                                            0xffffd5d0
          int main(){
0x0804845d
                                                            0xffffd5d4
               int a = 3, b = 5, c = 7;
                                                            0xffffd5d8
               f(a,b);
0 \times 08048488
                                                            0xffffd5dc
               g(b,c);
0x08048496
                                                            0xffffd5e0
                                                                                  5
               return 0;
                                                            0xffffd5e4
                                                            0xffffd5e8
```



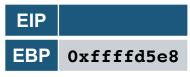
```
int f1(int fx1, int fy1, int fz1){
0x080483f6
               int fa1 = 20;
               return fa1;
           int f(int fx, int fy){
0 \times 08048412
                                                           Resets the previous EBP
               int fa = 10, fb = 12;
               f1(fx, fy, fa);
0x08048439
               return fb;
                                                            0xffffd5bc
                                                            0xffffd5c0
                                                                                 12
                                                            0xffffd5c4
                                                                                 10
           int g(int gx, int gy){
0x08048446
                                                                            0xffffd5e8
                                             EBP
                                                            0xffffd5c8
               return gx + gy;
                                                            0xffffd5cc
                                                                            0x0804848d
                                                            0xffffd5d0
          int main(){
0x0804845d
                                                            0xffffd5d4
               int a = 3, b = 5, c = 7;
                                                            0xffffd5d8
               f(a,b);
0 \times 08048488
                                                            0xffffd5dc
               g(b,c);
0x08048496
                                                            0xffffd5e0
                                                                                  5
               return 0;
                                                            0xffffd5e4
                                                            0xffffd5e8
```



```
int f1(int fx1, int fy1, int fz1){
0x080483f6
               int fa1 = 20;
               return fa1;
           int f(int fx, int fy){
0 \times 08048412
                                                           Resets the previous EBP
               int fa = 10, fb = 12;
               f1(fx, fy, fa);
0x08048439
               return fb;
                                                            0xffffd5c0
                                                                                 12
                                                            0xffffd5c4
                                                                                 10
           int g(int gx, int gy){
0x08048446
                                                            0xffffd5c8
                                                                             0xffffd5e8
                                             EBP
               return gx + gy;
                                                            0xffffd5cc
                                                                             0x0804848d
                                                            0xffffd5d0
          int main(){
0x0804845d
                                                            0xffffd5d4
               int a = 3, b = 5, c = 7;
                                                            0xffffd5d8
               f(a,b);
0 \times 08048488
                                                            0xffffd5dc
               g(b,c);
0x08048496
                                                            0xffffd5e0
                                                                                  5
               return 0;
                                                            0xffffd5e4
                                                            0xffffd5e8
```



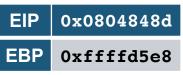
```
int f1(int fx1, int fy1, int fz1){
0x080483f6
               int fa1 = 20;
               return fa1;
           int f(int fx, int fy){
0 \times 08048412
                                                           Resets the previous EBP
               int fa = 10, fb = 12;
               f1(fx, fy, fa);
0x08048439
               return fb;
                                                            0xffffd5c0
                                                                                  12
                                                            0xffffd5c4
                                                                                 10
           int g(int gx, int gy){
0x08048446
                                                            0xffffd5c8
                                                                             0xffffd5e8
                                             EBP
               return qx + qy;
                                                            0xffffd5cc
                                                                             0x0804848d
                                                            0xffffd5d0
           int main(){
0x0804845d
                                                            0xffffd5d4
               int a = 3, b = 5, c = 7;
                                                            0xffffd5d8
               f(a,b);
0 \times 08048488
                                                            0xffffd5dc
               g(b,c);
0x08048496
                                                            0xffffd5e0
                                                                                  5
               return 0;
                                                            0xffffd5e4
                                             EBP
                                                            0xffffd5e8
```



```
int f1(int fx1, int fy1, int fz1){
0x080483f6
                int fa1 = 20;
                return fa1;
           int f(int fx, int fy){
0x08048412
                int fa = 10, fb = 12;
                f1(fx, fy, fa);
0x08048439
                return fb;
           int q(int qx, int qy){
0x08048446
                return gx + gy;
           int main(){
0x0804845d
                int a = 3, b = 5, c = 7;
                f(a,b);
0 \times 08048488
                g(b,c);
0x08048496
                return 0;
                                                EBP
```

#### Resets the previous EBP

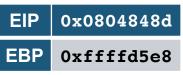
0xffffd5c0	12
0xffffd5c4	10
0xffffd5c8	0xffffd5e8
0xffffd5cc	0x0804848d
0xffffd5d0	3
0xffffd5d4	5
0xffffd5d8	
0xffffd5dc	7
0xffffd5e0	5
0xffffd5e4	3
0xffffd5e8	



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

#### **Continues where it** stoped in main

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



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

#### **Continues where it** stoped in main

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



```
int f1(int fx1, int fy1, int fz1){
0x080483f6
                int fa1 = 20;
                return fa1;
           int f(int fx, int fy){
0x08048412
                int fa = 10, fb = 12;
                f1(fx, fy, fa);
0x08048439
                return fb;
           int q(int qx, int qy){
0x08048446
                return gx + gy;
           int main(){
0x0804845d
                int a = 3, b = 5, c = 7;
                f(a,b);
0 \times 08048488
                g(b,c);
0x08048496
                return 0;
                                                EBP
```

#### And the frame of f **Becomes unused**

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



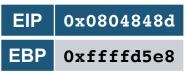
```
int f1(int fx1, int fy1, int fz1){
0x080483f6
                int fa1 = 20;
                return fa1;
           int f(int fx, int fy){
0x08048412
                int fa = 10, fb = 12;
                f1(fx, fy, fa);
0x08048439
                return fb;
           int g(int gx, int gy){
0x08048446
                return gx + gy;
           int main(){
0x0804845d
                int a = 3, b = 5, c = 7;
                f(a,b);
0 \times 08048488
                g(b,c);
0x08048496
                return 0;
```

And the frame of f **Becomes unused** 

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



```
int f1(int fx1, int fy1, int fz1){
0x080483f6
               int fa1 = 20;
               return fa1;
           int f(int fx, int fy){
0x08048412
               int fa = 10, fb = 12;
               f1(fx, fy, fa);
0x08048439
               return fb;
           int g(int gx, int gy){
0x08048446
               return gx + gy;
                                                                     Repeat for g
           int main(){
0x0804845d
               int a = 3, b = 5, c = 7;
                                                              0xffffd5d8
               f(a,b);
0 \times 08048488
                                                              0xffffd5dc
               g(b,c);
0x08048496
                                                              0xffffd5e0
                                                                                     5
               return 0;
                                                              0xffffd5e4
                                              EBP
                                                              0xffffd5e8
```



```
int f1(int fx1, int fy1, int fz1){
0x080483f6
               int fa1 = 20;
               return fa1;
           int f(int fx, int fy){
0x08048412
               int fa = 10, fb = 12;
               f1(fx, fy, fa);
0x08048439
               return fb;
           int q(int qx, int qy){
0x08048446
               return gx + gy;
                                                                     Repeat for g
           int main(){
0x0804845d
               int a = 3, b = 5, c = 7;
               f(a,b);
0 \times 08048488
                                                              0xffffd5dc
               g(b,c);
0x08048496
                                                              0xffffd5e0
                                                                                     5
               return 0;
                                                              0xffffd5e4
                                              EBP
                                                              0xffffd5e8
```