C++ Tricks 2.4 I386C

farseerfc.wordpress.com

2.4 I386C

(eip)ebp()

32intshortchareax64
_int64edx+eaxedx32eax32float
doubleC++

```
void f(){
int i=g(1,2);
}
int g(int a,int b){
int c=a+b
return c;
}

f:
push ebp ;ebp
mov ebp,esp ;
sub esp,4 ;i
mov eax,2 ;b2
push eax ;b
mov eax,1 ;a1
push eax ;a
```

```
call g ;g
add esp,8 ;ab
mov dword ptr[ebp-4],eax ;i
mov esp,ebp ;
pop ebp ;
g:
push ebp ;ebp
mov ebp,esp ;
sub esp,4 ;c
mov eax,dword ptr[ebp+8] ;ebpa
mov ebx,dword ptr[ebp+12] ;ebpb
add eax,ebx ;abeax
mov dword ptr[ebp-4],eax ;c
mov eax,dword ptr[ebp-4] ;c
add esp,4 ;c
mov esp,ebp ;
pop ebp ;
ret ;f
```

100076:c <- gesp

100080:febp=100100 <- gebp

100084:feip

100088:a=1

100092:b=2

100096:i

100100:ebp <-febp

100104:……

gebpebp32ebp-4ebp-832 ebp+8ebp+1232

CintC++C++void C++