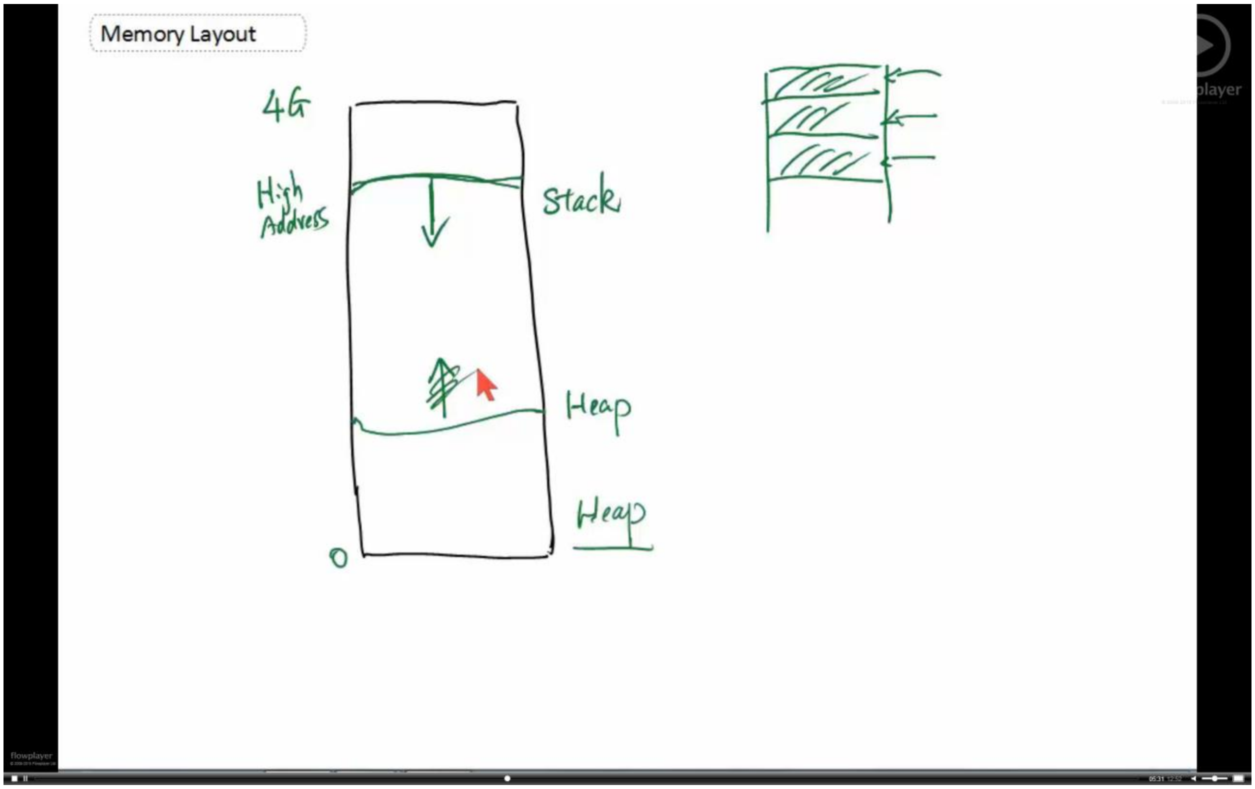
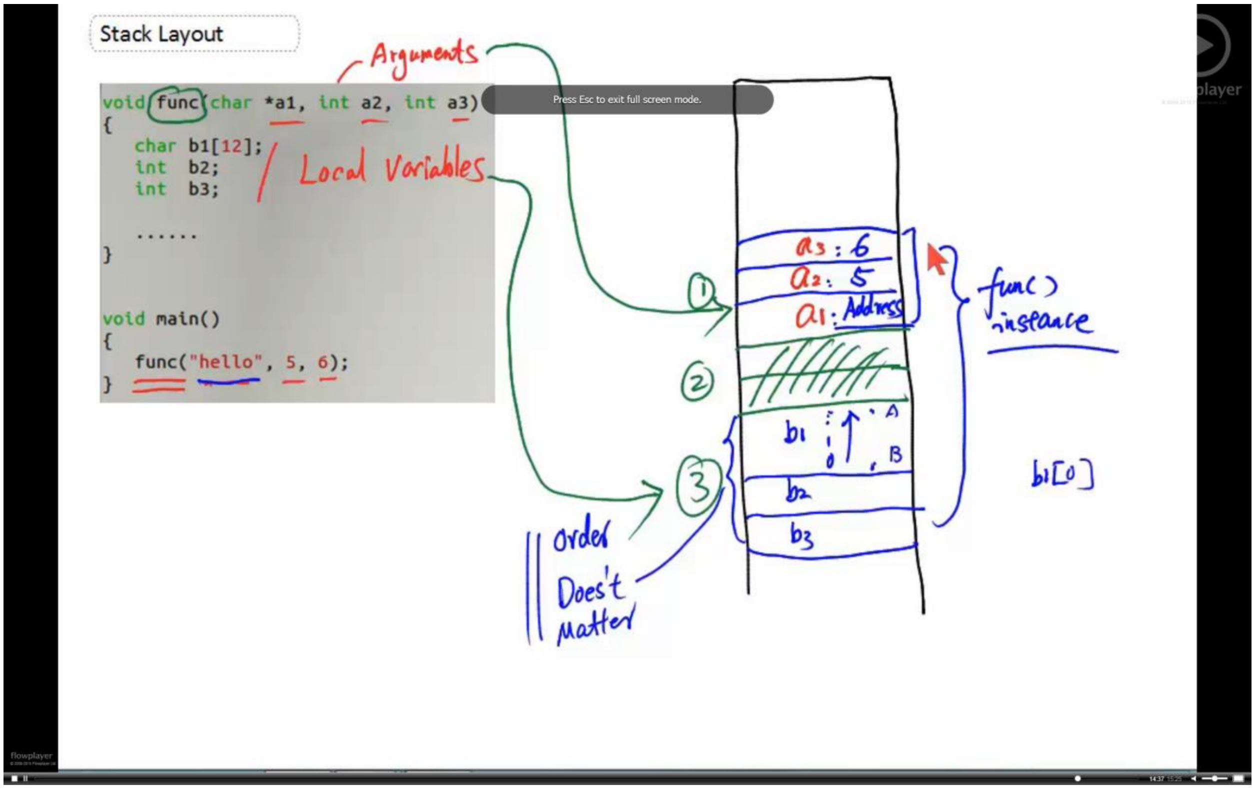


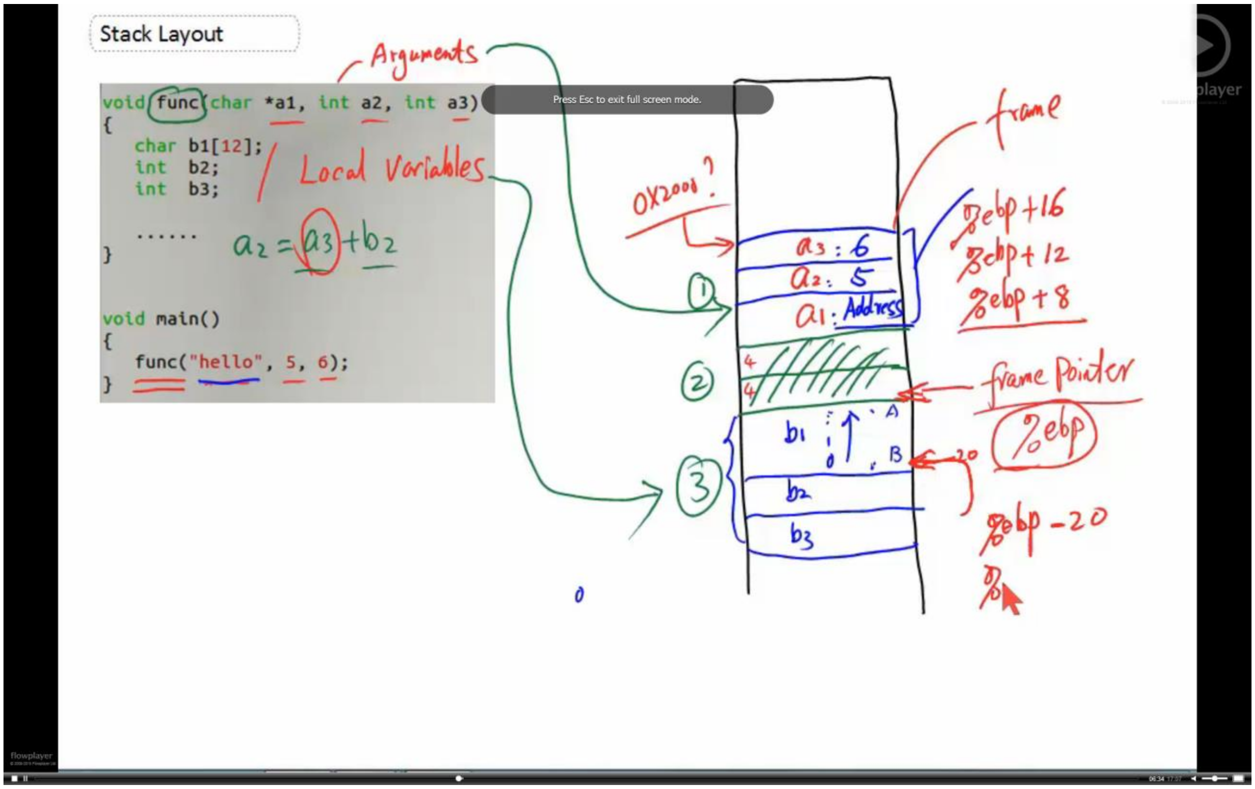
Memory Layout



Stack Layout

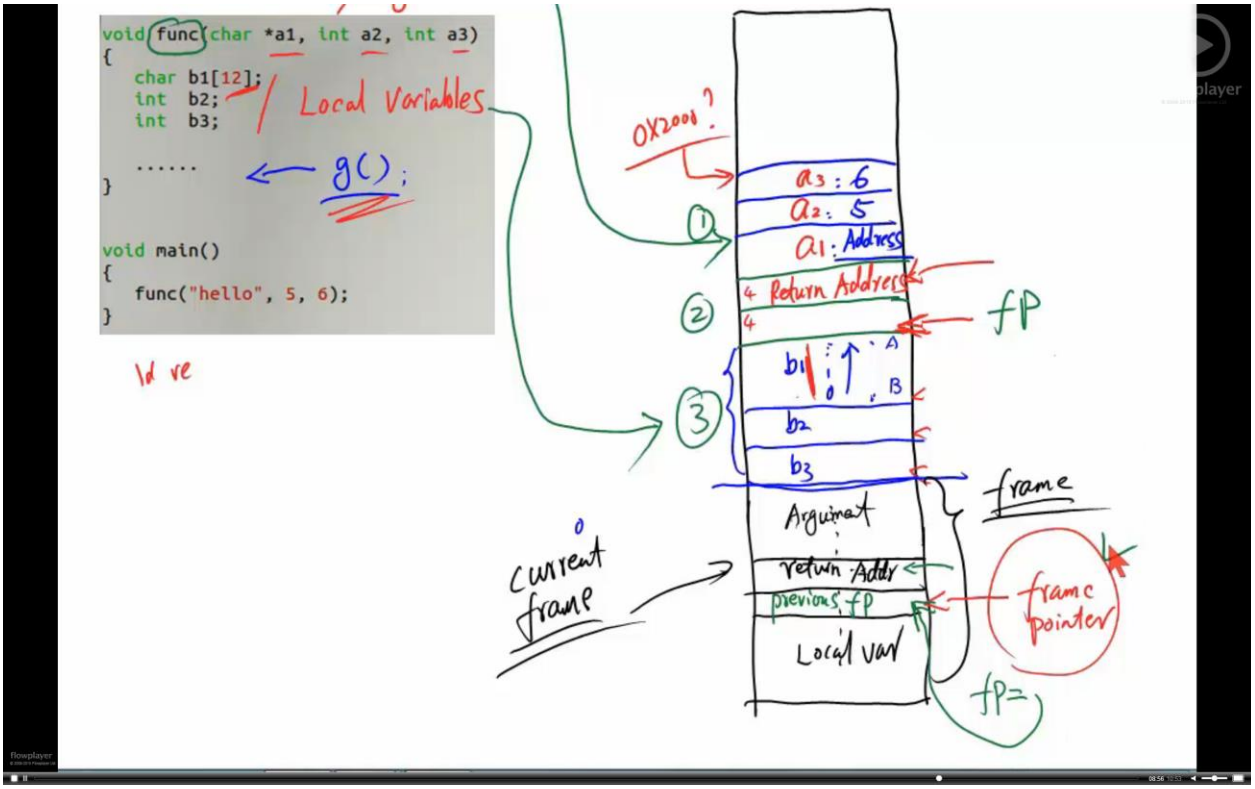
```
void func(char *a1, int a2, int a3)
{
   char b1[12];
   int  b2;
   int  b3;

   ......
}

void main()
{
   func("hello", 5, 6);
}
```

Press Esc to exit full screen mode.

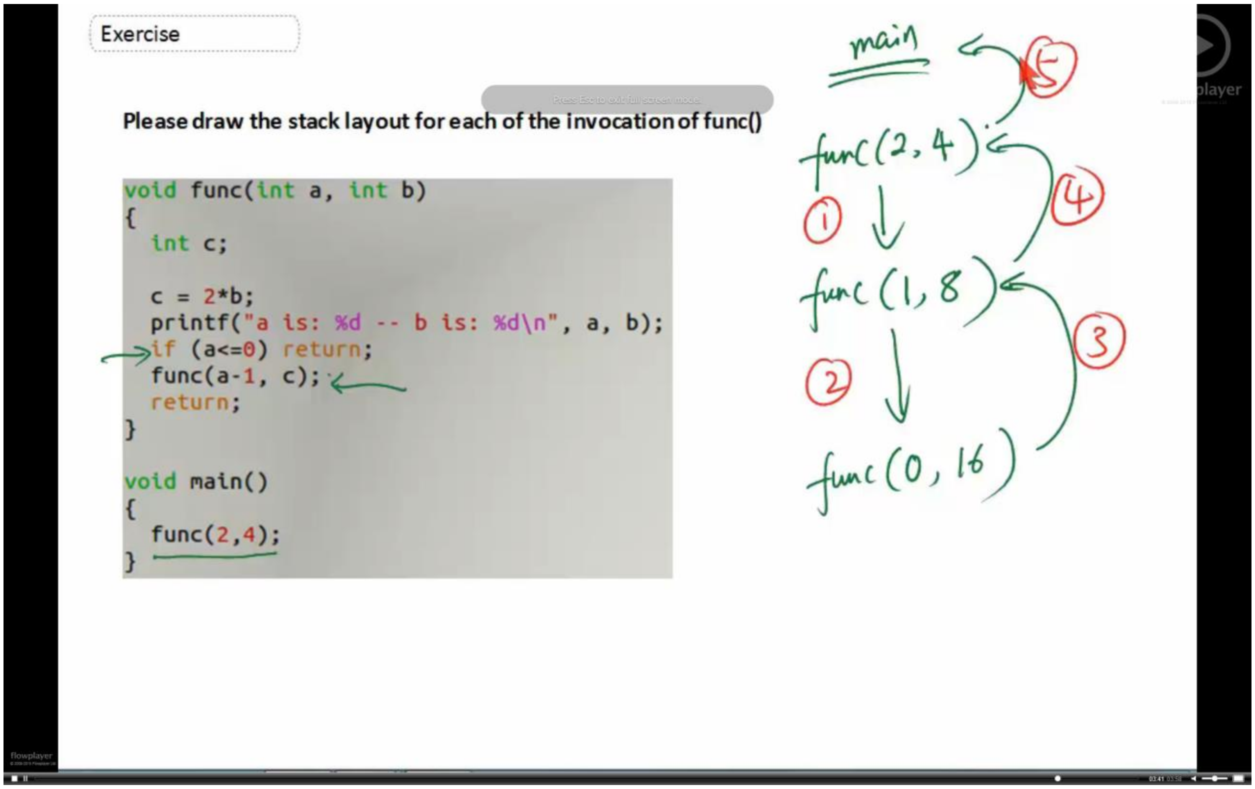


Stack Layout

```
void func(char *a1, int a2, int a3)
{
   char b1[12];
   int b2;
   int b3;

   ......
}

void main()
{
   func("hello", 5, 6);
}
```



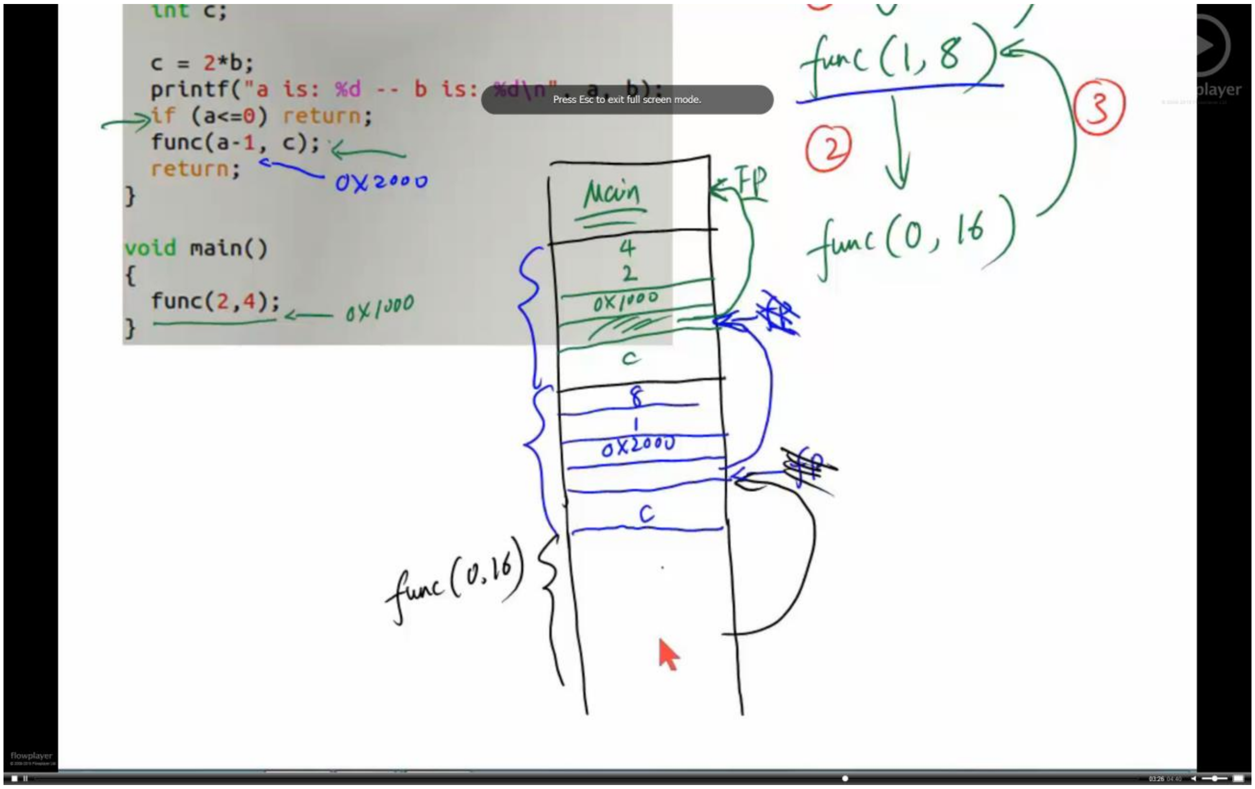
```
void func(char *a1, int a2, int a3)
{
   char b1[12];
   int b2;
   int b3;

   ......
}

void main()
{
   func("hello", 5, 6);
}
```



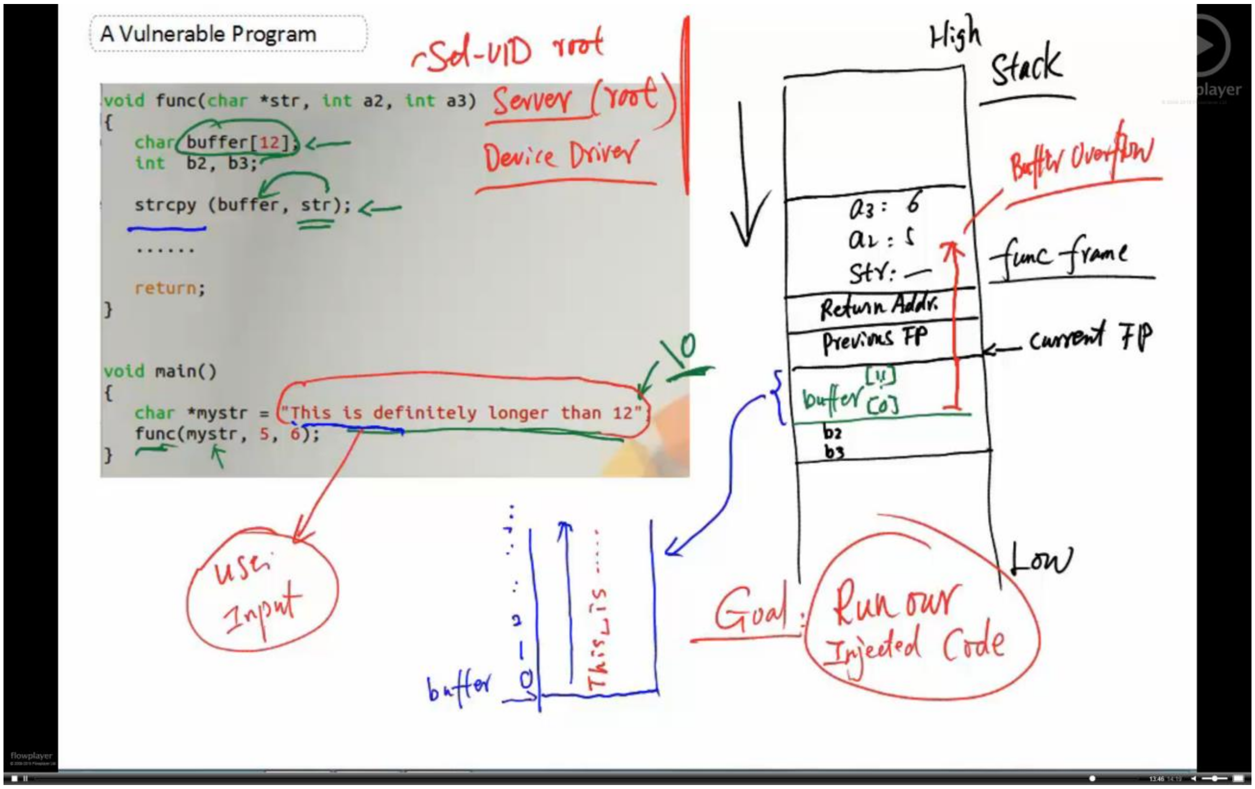
Exercise

Please draw the stack layout for each of the invocation of func()

```
void func(int a, int b)
{
  int c;

  c = 2*b;
  printf("a is: %d -- b is: %d\n", a, b);
  if (a<=0) return;
  func(a-1, c);
  return;
}

void main()
{
  func(2,4);
}
```

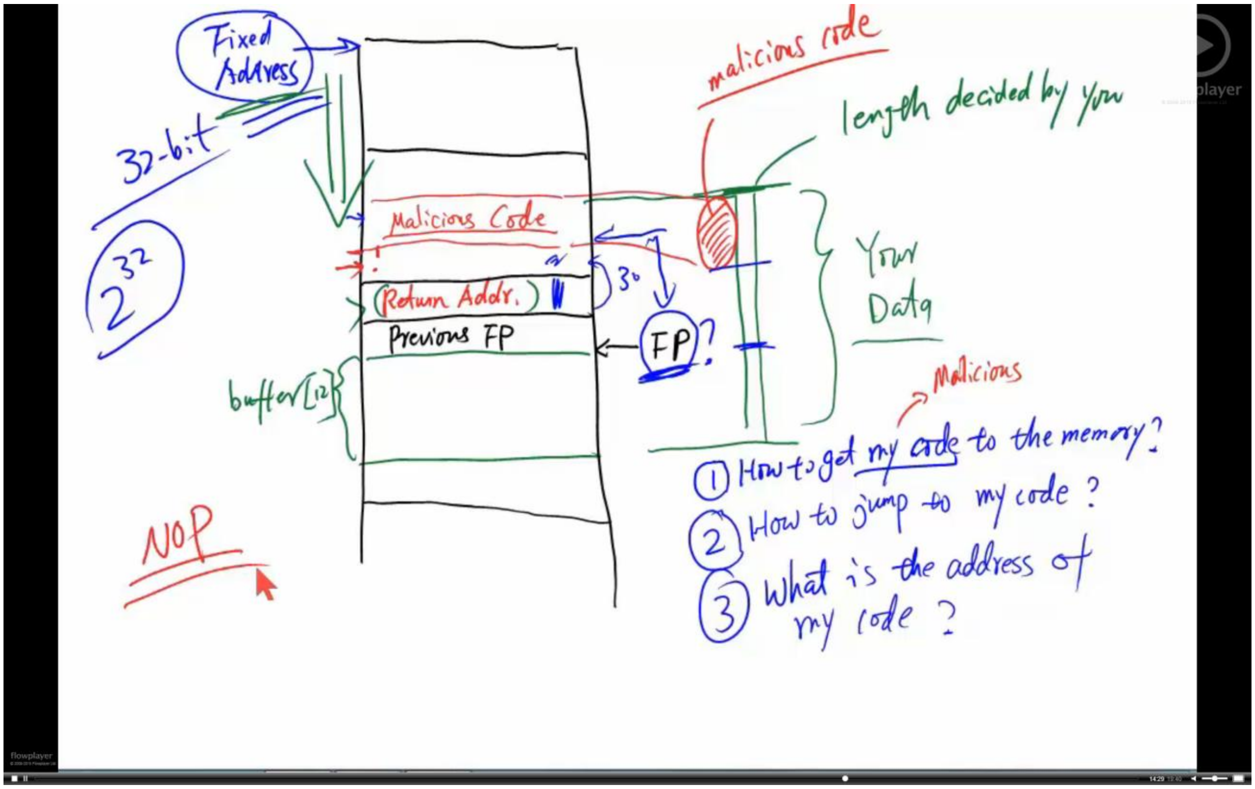


```
  int c;

  c = 2*b;
  printf("a is: %d -- b is: %d\n", a, b);
  if (a<=0) return;
  func(a-1, c);
  return;
}

void main()
{
  func(2,4);
}
```



A Vulnerable Program

```
void func(char *str, int a2, int a3)
{
    char buffer[12];
    int  b2, b3;

    strcpy (buffer, str);
    ......

    return;
}

void main()
{
    char *mystr = "This is definitely longer than 12";
    func(mystr, 5, 6);
}
```



1. How to get my code to the memory?
2. How to jump to my code?
3. What is the address of my code?