```
void function(int a, int b, int c){
  char buffer1[5];
  char buffer2[1];
}
int main(int argc, char **argv){
  function(1,2,3);
}

Parameters
  for main

return Address

prev frame pointer

Locals of main

Parameters
  for function

return Address

prev frame pointer

Locals of function

Stack pointer
```

Stack Usage Contd.

```
void function(int a, int b, int c)
{
         char buffer1[5];
         char buffer2[10];
}
void main()
{
         function(1,2,3);
}
```

What is the output of the following?

- printf("%x", buffer2) : 966
- printf("%x", &buffer2[10])
 976 → buffer1

Therefore buffer2[10] = buffer1[0]

A BUFFER OVERFLOW

Stack (top to bottom):	
address	stored data
1000 to 997	3
996 to 993	2
992 to 989	1
988 to 985	return address
988 to 985 984 to 981	return address %ebp (stored frame pointer)
	%ebp (stored
984 to 981	%ebp (stored frame pointer)