<Cykor 1주차 과제 보고서>

2025350013 최효석

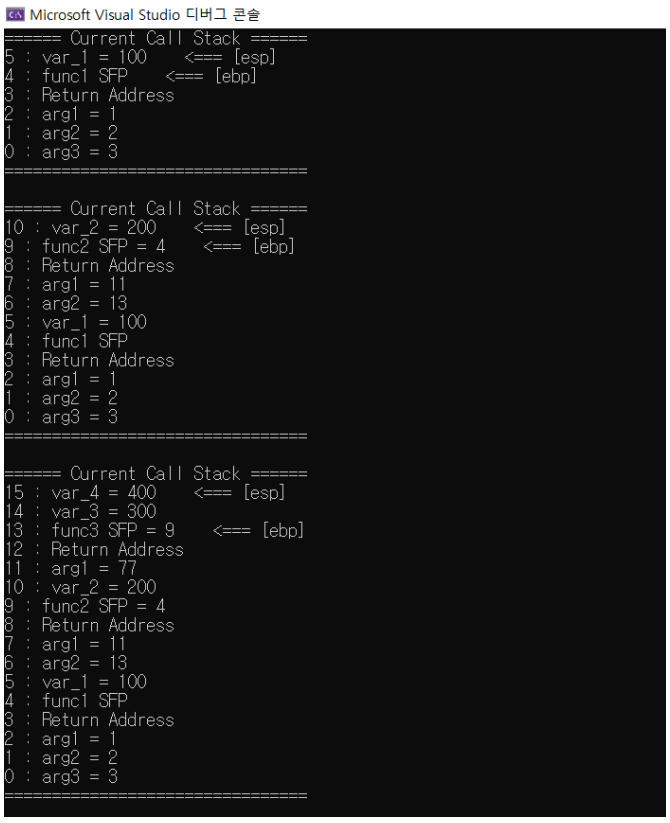
개요

C 언어에서 함수가 실행되고 종료될 때 스택 메모리에서 발생하는 과정을 설명합니다. 특히, 함수의 프롤로그와 에필로그에서 스택 메모리에 데이터를 푸시(push)하고 팝(pop)하는 과정을 중심으로 설명합니다. 예시 코드로는 main, func1, func2, func3 함수가 사용됩니다.

함수 프롤로그

함수가 호출될 때, 스택 프레임을 형성하기 위해 여러 데이터를 스택에 순서대로 푸시합니다. 이 과정은 함수의 프롤로그라고 불리며, 다음과 같은 단계로 이루어집니다:

1. 매개변수 푸시: 함수의 매개변수들이 스택에 푸시됩니다.
2. 반환 주소 푸시: 함수가 종료된 후 돌아갈 주소가 스택에 푸시됩니다.
3. 저장된 프레임 포인터(SFP) 푸시: 이전 함수의 프레임 포인터가 스택에 푸시됩니다.
4. 지역 변수 푸시: 함수 내에서 사용되는 지역 변수들이 스택에 푸시됩니다.



<- 전체 함수 프롤로그 과정

Microsoft Visual Studio 디버그 콘솔

```
====== Current Call Stack ======
5 : var_1 = 100     <=== [esp]
4 : func1 SFP     <=== [ebp]
3 : Return Address
2 : arg1 = 1
1 : arg2 = 2
0 : arg3 = 3
================================
```

func1의 함수 프롤로그(main함수는 표현하지 않음)

매개변수,반환주소값,SFP,지역변수 순으로 메모리에 저장되며, 매개변수의 경우 오른쪽에서부터 저장된다.

```
====== Current Call Stack ======
10 : var_2 = 200    <=== [esp]
9 : func2 SFP = 4    <=== [ebp]
8 : Return Address
7 : arg1 = 11
6 : arg2 = 13
5 : var_1 = 100
4 : func1 SFP
3 : Return Address
2 : arg1 = 1
1 : arg2 = 2
0 : arg3 = 3
================================
```

func2의 함수 프롤로그

SP를 최상단으로 올리고, 이전의 FP를 새로 올린 스택프레임의 SFP에 저장하고 FP를 새로 올린 스택프레임의 SFP의 위치로 변경

```
====== Current Call Stack ======
15 : var_4 = 400    <=== [esp]
14 : var_3 = 300
13 : func3 SFP = 9     <=== [ebp]
12 : Return Address
11 : arg1 = 77
10 : var_2 = 200
9 : func2 SFP = 4
8 : Return Address
7 : arg1 = 11
6 : arg2 = 13
5 : var_1 = 100
4 : func1 SFP
3 : Return Address
2 : arg1 = 1
1 : arg2 = 2
0 : arg3 = 3
================================
```

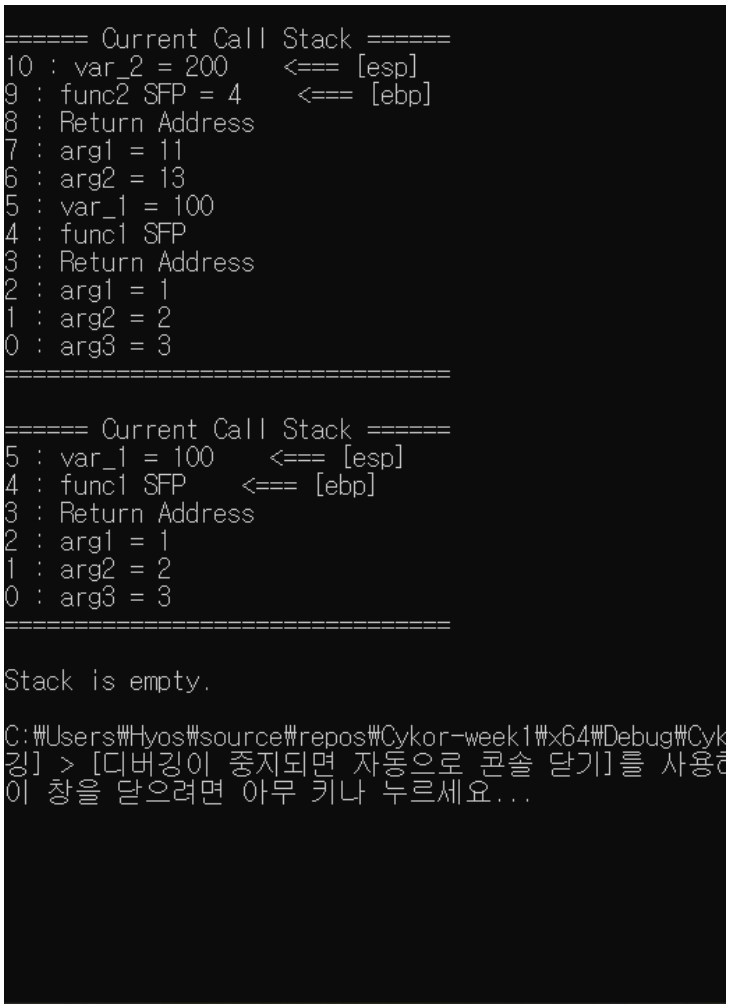
func3의 함수 프롤로그

func2의 스택프레임을 올릴 때와 유사하게 SFP에 이전 FP 위치를 저장하고 FP와 SP 갱신

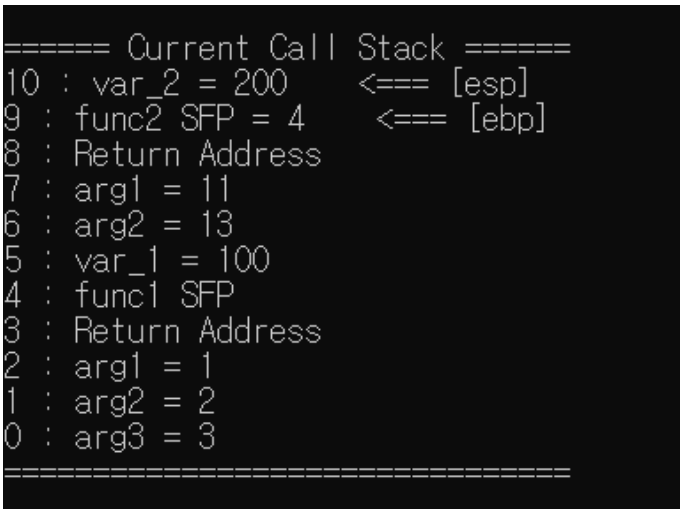
함수 에필로그

함수가 종료될 때, 스택 프레임을 제거하기 위해 여러 데이터를 스택에서 팝합니다. 이 과정은 함수의 에필로그라고 불리며, 다음과 같은 단계로 이루어집니다:

1. 지역 변수 팝: 함수 내에서 사용된 지역 변수들이 스택에서 팝됩니다.
2. 저장된 프레임 포인터(SFP) 팝: 저장되어 있던 이전 함수의 SFP 위치를 받아 FP 위치를 갱신하고, 종료되는 함수의 프레임 포인터가 스택에서 팝됩니다.
3. 반환 주소 팝: 함수가 종료된 후 돌아갈 주소가 스택에서 팝됩니다.
4. 매개변수 팝: 함수가 종료되고 값이 반환될 때, 함수의 매개변수들이 스택에서 팝됩니다.

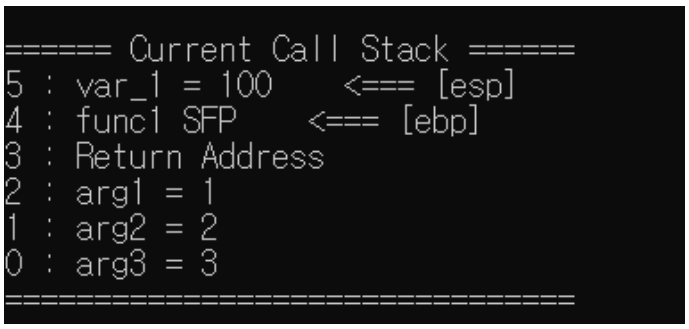


<- 함수 프롤로그 과정



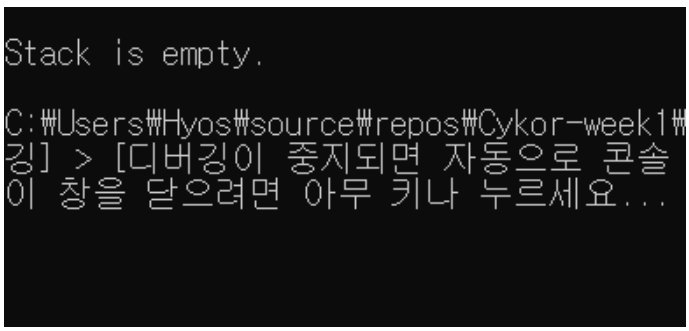
func3의 스택프레임 제거

func3의 SFP 값으로 FP를 갱신하여 ebp를 9번째인 func2의 SFP 위치로 지정하고 위에서부터 pop하여 매개변수까지 pop된 후 SP는 func2의 최상단인 10번째로 갱신된다



func2의 스택프레임 제거

func3의 스택프레임을 제거할 때와 유사하다. 종료되는 함수의 SFP 값으로 FP를 조정하고 제거된 후엔 SP가 5번째로 조정된다.



func1의 스택프레임 제거

func1의 값을 반환하고 func1의 스택프레임을 제거한다. 지역변수, SFP, 반환주소값, 매개변수 순으로 제거되어 stack의 메모리가 전부 휘발된다.

결론

이 보고서는 C 언어에서 함수가 실행되고 종료될 때 스택 메모리에서 발생하는 과정을 설명했습니다. 함수의 프롤로그와 에필로그에서 데이터를 푸시하고 팝하는 과정을 통해 스택 메모리가 어떻게 사용되는지 이해할 수 있었습니다. 스택의 일시적인 데이터 저장 특징을 이 활동을 통해 이해하고, 이러한 과정이 메모리의 일관성을 유지하고, 프로그램의 안정성을 보장하는 데 중요한 역할을 한다는 것을 알았습니다.