Calling Convention

Code Cave

Lena tutorial #15

김건희

Calling Convention (함수 호출 규약)

함수를 호출할 때 인자를
전달하는 방식이나 함수
실행이 끝나고 스택에
정리하는 방식에 대한 약속

- cdecl
- stdcall
- fastcall

Calling Convention (함수 호출 규약)

>고급언어

```
void caller() {
  callee(1,2);
  return;
}
```

↓

```
[caller]
PUSH 2
PUSH 1
CALL callee
ADD ESP 8
```

```
[callee]
X
```

인자 전달 방법 : 스택
인자 전달 순서 : 오른 -> 왼
스택 정리 : 호출자 -> 피호출자

cdecl

stdcall

fastcall

Calling Convention (함수 호출 규약)

>고급언어

```
void caller() {
  callee(1,2);
  return;
}
```

↓

```
[caller]
PUSH 2
PUSH 1
CALL callee
.....
```

```
[callee]
PUSH EBP
MOV EBP, ESP
.....
POP EBP
RETN 8
```

인자 전달 방법 : 스택
인자 전달 순서 : 오른 -> 왼
스택 정리 : 피호출자

cdecl

stdcall

fastcall

Calling Convention (함수 호출 규약)

>고급언어

```
void caller() {
  callee(1,2);
  return;
}
```

↓

```
[caller]
MOV EDX 2
MOV ECX 1
CALL callee
.........
```

인자 전달 방법 : 레지스터, 스택
인자 전달 순서 : ECX, EDX 레지스터로 전달 후 스택 (오른 -> 왼)
스택 정리 : X (레지스터를 사용하기 때문)

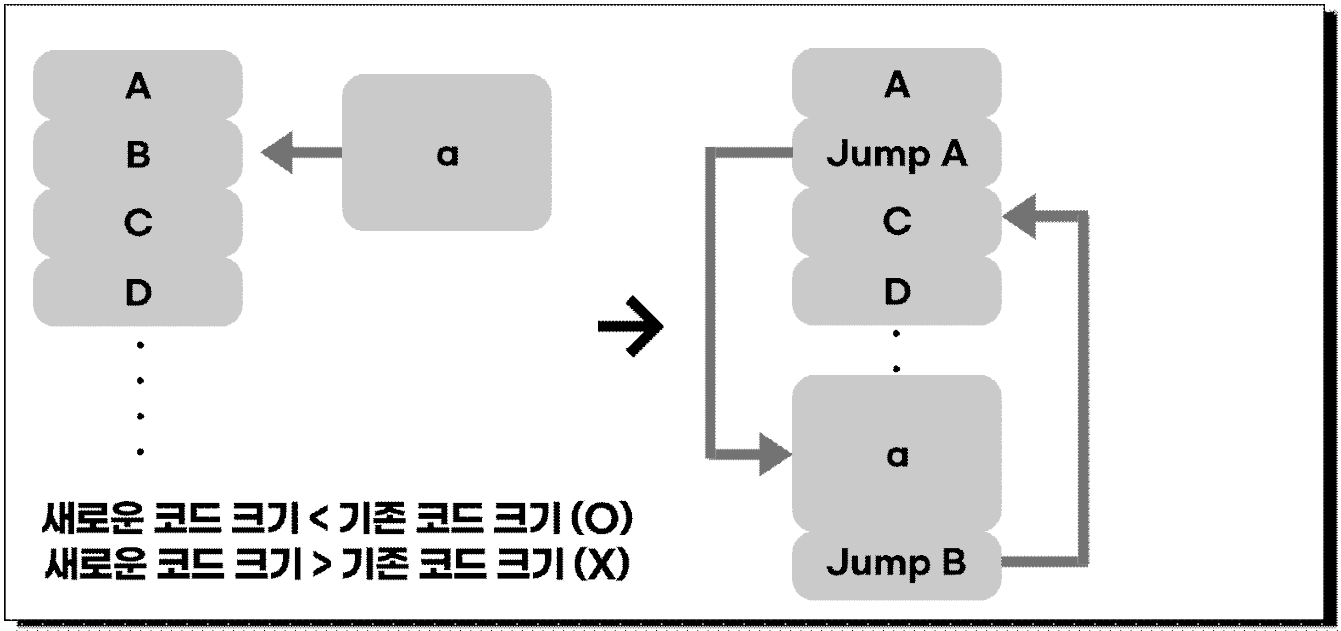
```
[callee]
PUSH EBP
MOV EBP, ESP
.........
MOV DWORD PTR SS:[EBP-8],EDX
MOV DWORD PTR SS:[EBP-4],ECX
.........
POP EBP
RETN
```

cdecl

stdcall

fastcall

Code Cave (코드 케이브)

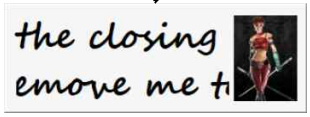


Lena Tutorial #15

1

2

3



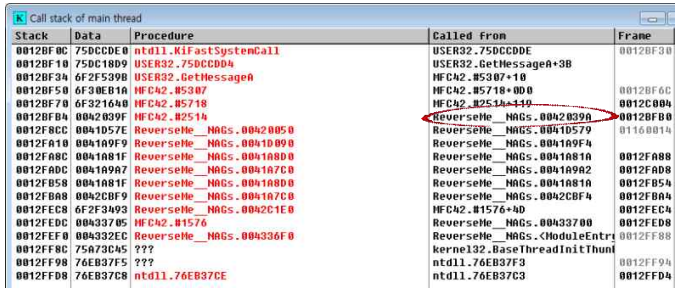
목표 : Nag 창 없애기

1, 3 - Nag 창
2 - 정상 창

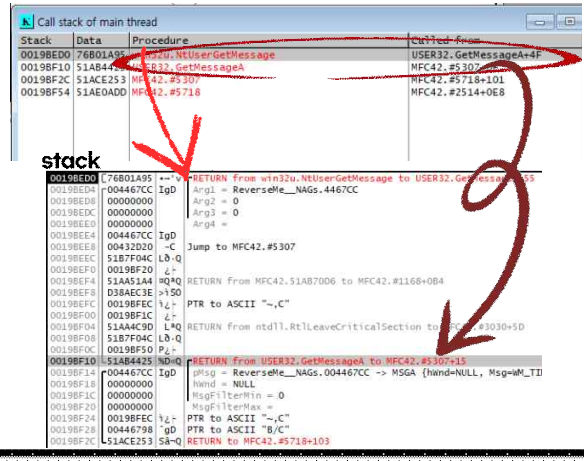
Lena Tutorial #15

Call stack window : 콜 스택들을 모아서 보여줌

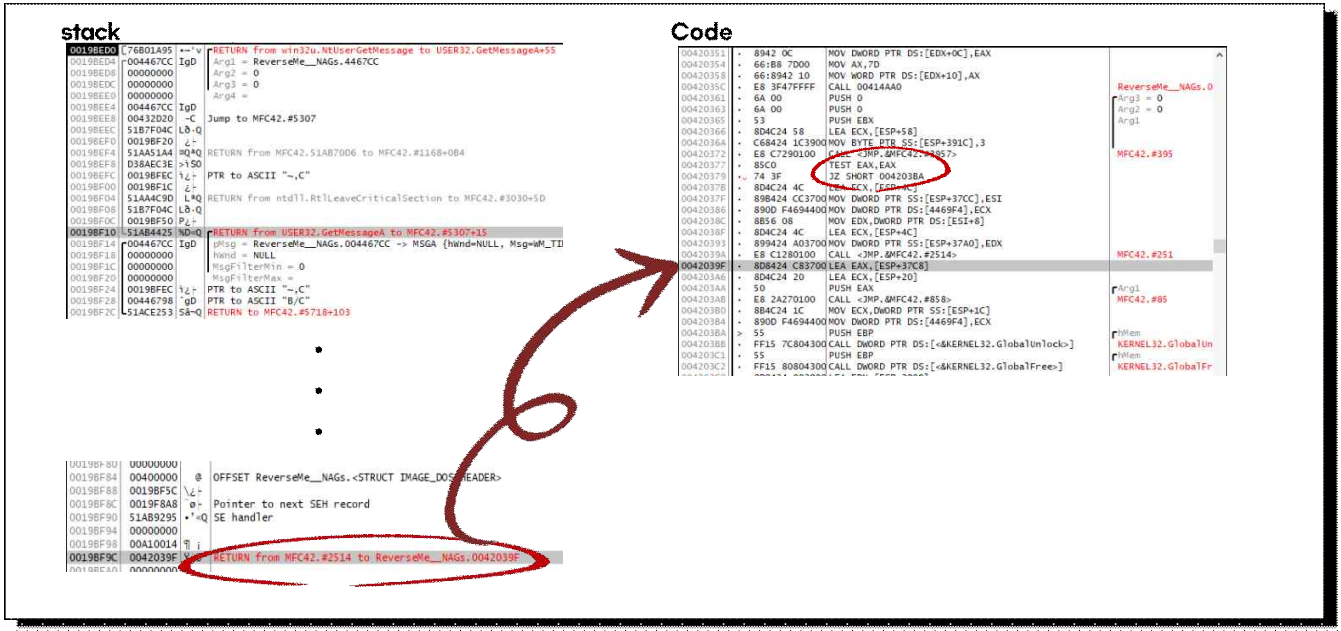
정상



?



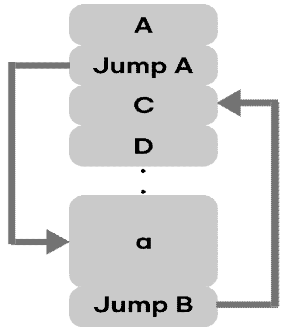
Lena Tutorial #15



Lena Tutorial #15

Code

```
00420377   E9 EE790100   JMP 00437D6A
0042037C   90            NOP
0042037D   90            NOP
0042037E   90            NOP
0042037F   89B424 CC3700 MOV DWORD PTR SS:[ESP+37CC],ESI
                  •
                  •
00437D6A   0005 905E4400 ADD BYTE PTR DS:[445E90],AL
00437D70   803D 905E4400 CMP BYTE PTR DS:[445E90],2
00437D77   0F85 3D86FEFF JNE 004203BA
00437D7D   8D4CE4 4C     LEA ECX,[ESP+4C]
00437D81   E9 F985FEFF   JMP 0042037F
00437D86   00            DB 00
00437D87   00            DB 00
```



445E90에 AL값을 더함
AL 값이 2가 되었을때 창을 보여줌

End