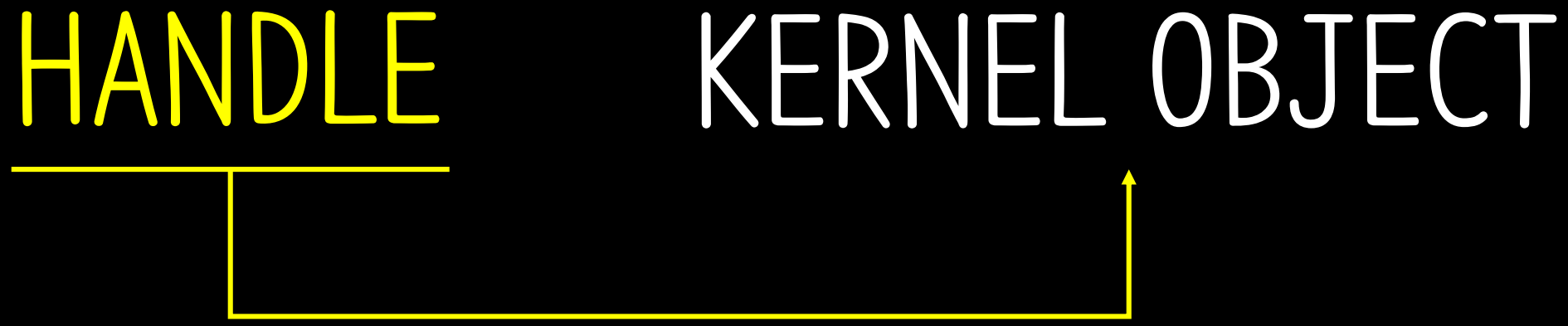

18.08.02 # pinebudweiser
More Deeply
HANDLE


HANDLE
KERNEL OBJECT

핸들에 대해 아시나요?

핸들의 값이 11(dec)이 될 수 있을까요?

핸들의 값은 중복 될 수 있을까요?

핸들은 몇 개가 생성 될 수 있을까요?

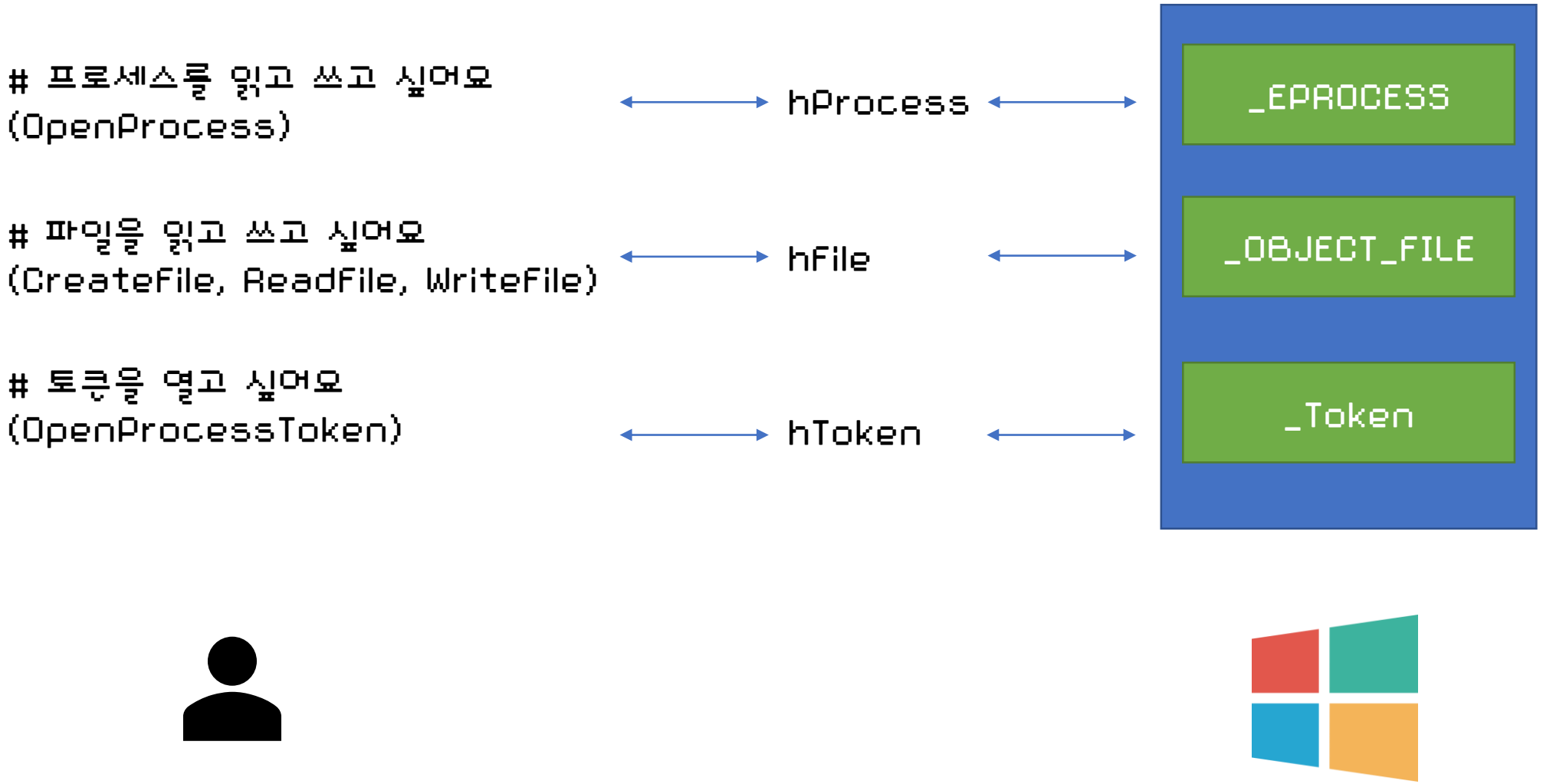
핸들에 대해 아시나요?

핸들의 값이 11(dec)이 될 수 있을까요? 아뇨

핸들의 값은 중복 될 수 있을까요? 네

핸들은 몇 개가 생성 될 수 있을까요? 2^5*2^10*(2^9-1)

18.07.19 - Handle Hijacking




hProcess
00000020h
_EPROCESS
865C1898h

HANDLE Strucuter

EPROCESS

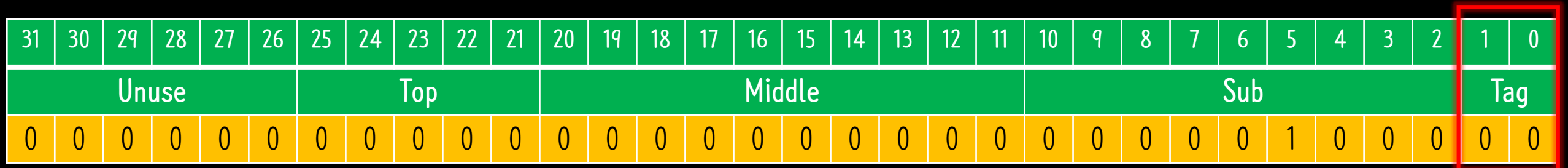
HANDLE_TABLE

HANDLE_TABLE_ENTRY

OBJECT_HEADER

Body

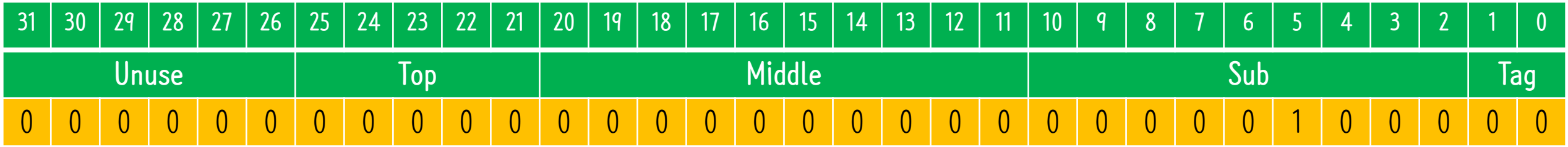
핸들의 구조

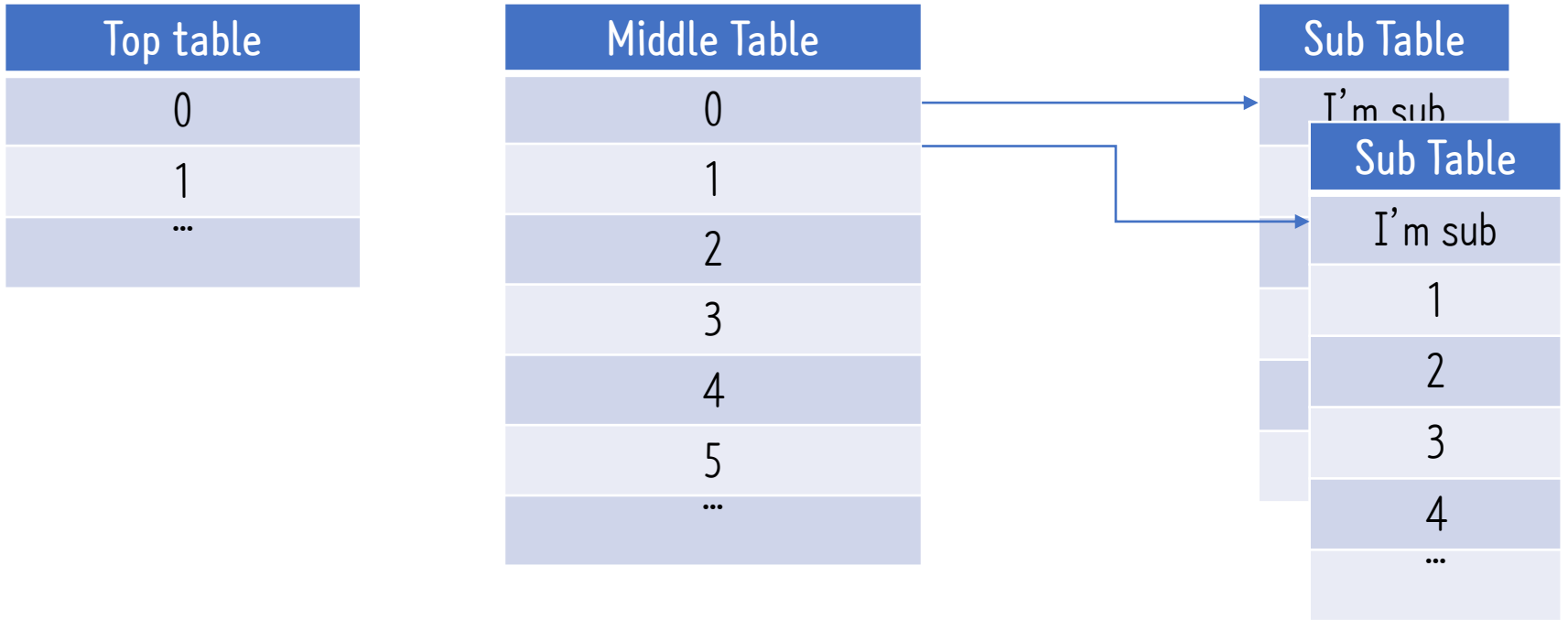


›› 이 녀석 때문에 핸들 값이 4씩 증가한다 =_=

[+] 인덱스를 계산 할 때도 (핸들 값/4)로 계산

핸들의 구조


31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
Unuse
Top
Middle
Sub
Tag
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0


Top table
0
1
…
Middle Table
0
1
2
3
4
5
…
Sub Table
I'm sub
Sub Table
I'm sub
1
2
3
4
…

HANDLE_TABLE -> TableCode

TableCode Structure

(HANDLE_TABLE_ENTRY | LevelIndex)

핸들이 어디까지 채워졌니?
0 - SubTable
1 - MiddleTable
2 - TopTable

Simple formula

LevelIndex = TableCode & 3
HANDLE_TABLE_ENTRY = TableCode & ~2

(중요) 레벨에 따라 가리키는 테이블이 틀려짐!

_HANDLE_TABLE_ENTRY

```
_HANDLE_TABLE_ENTRY Simple Struct{
        + OBJECT_HEADER_ADDRESS
        + GrantedAccess
}
```

OBJECT_HEADER_ADDRESS	A	I	L

Simple formula

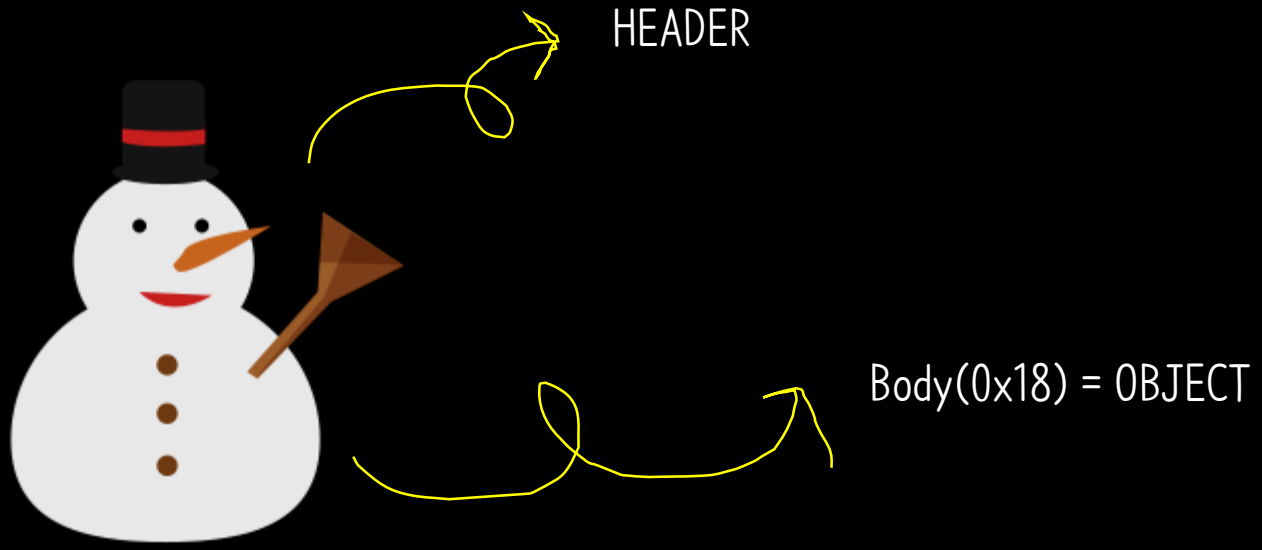
OBJECT_HEADER_ADDRESS = OBJECT_HEADER_ADDRESS & ~7

Flag explain

Lock bit – 핸들을 오브젝트 포인터로 변환 시, 변환중의 상태를 나타냄
Inherit bit – 부모 프로세스와 자식프로세스간 프로세스의 핸들 테이블을 상속 받을지의 여부
Audit bit – 오브젝트가 닫힐 때, 감사 메시지의 생성 여부(내부사용)

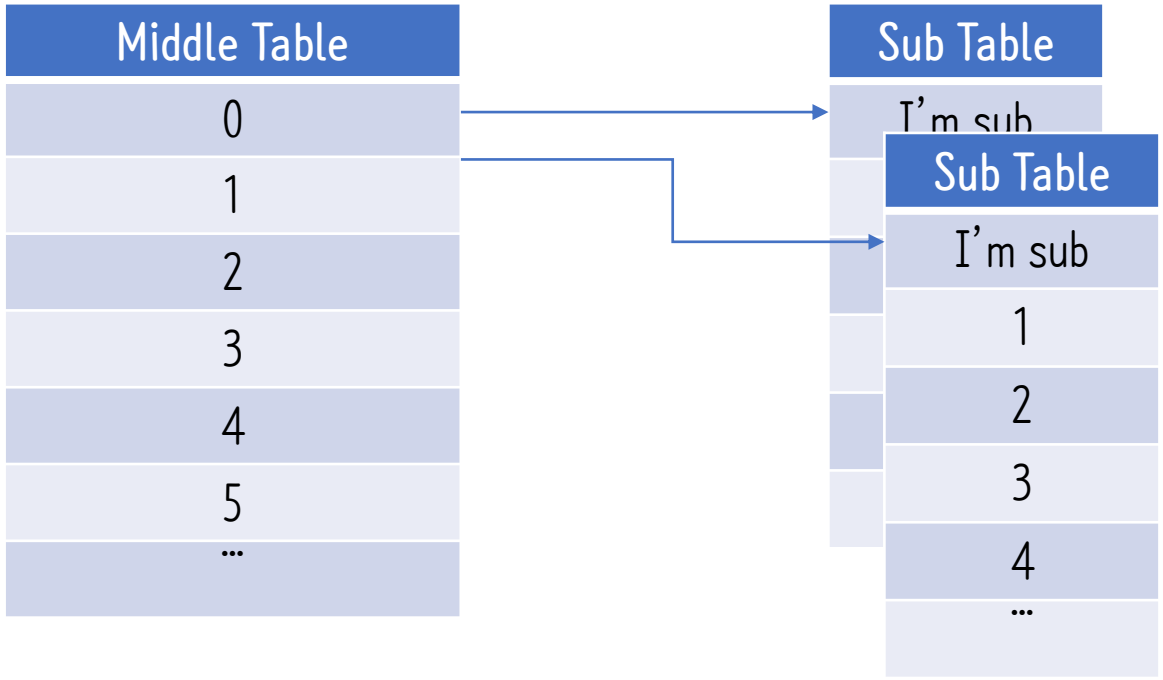
_OBJECT_HEDAER

_OBJECT_HEADER Structure



SHOW YOU

In this case



Any Questions?