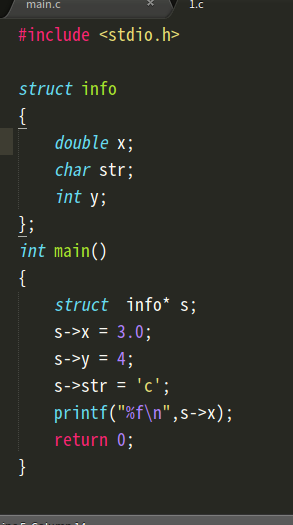
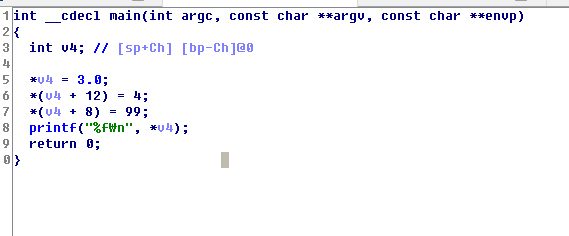


구조체가 포인터 형이 아닐 때에는 분석하기 어렵다고 판단하였고 구조체 주소를 참조하는 변수들을 살펴보기로 결정하였습니다.

- 

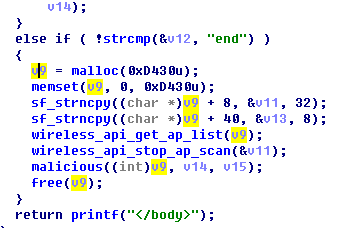
 **플러그인 사용**

<https://github.com/igogo-x86/HexRaysPyTools> 참조

**빨간색 = origin**

노랑색 = **충돌**



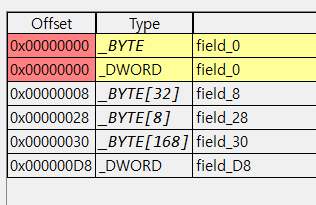


**V9**

8바이트

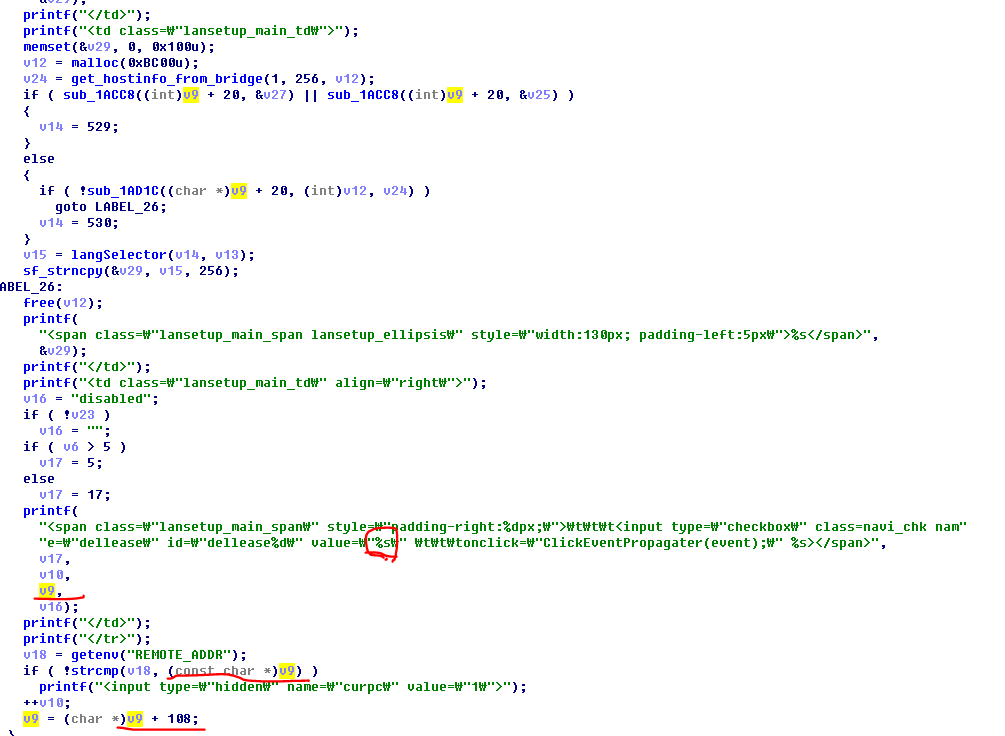
Char [32]

Char [8]





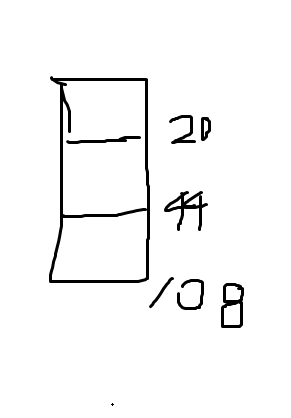




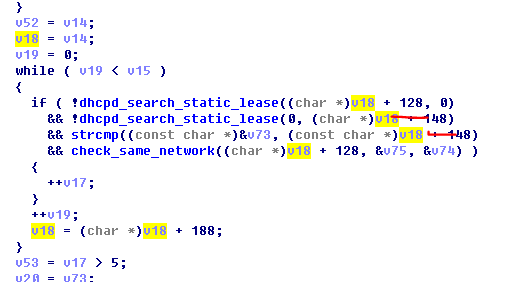
**Char [20]**

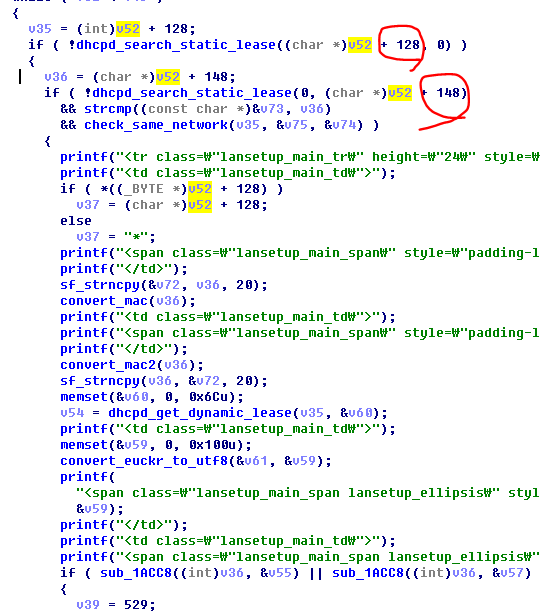
**Char [24]**

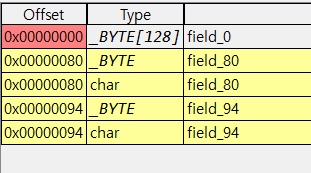
**Char[64](?)**

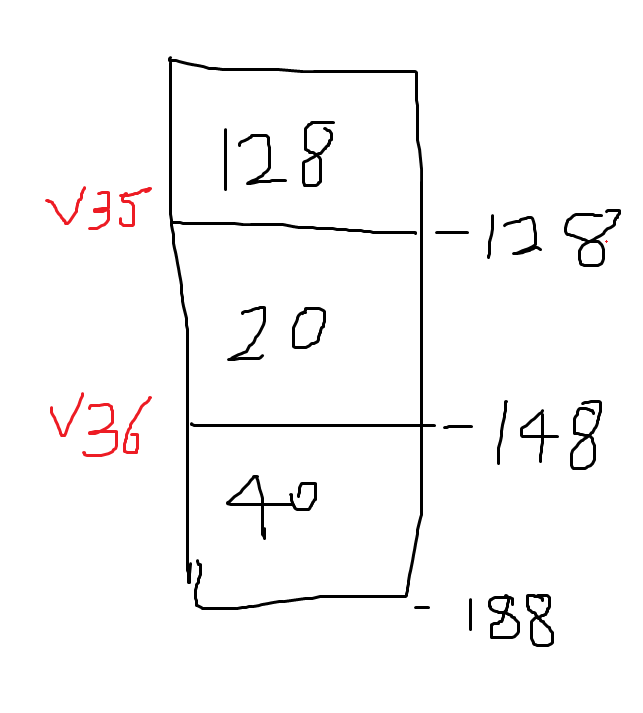




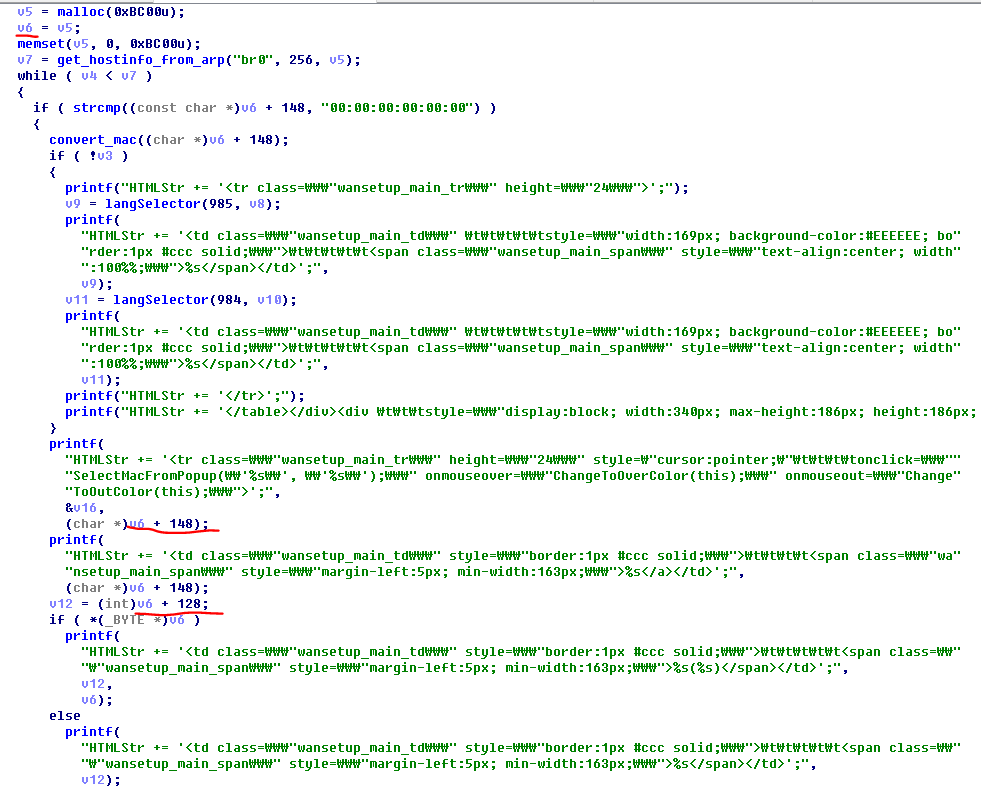






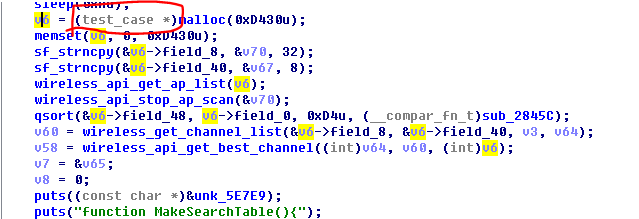


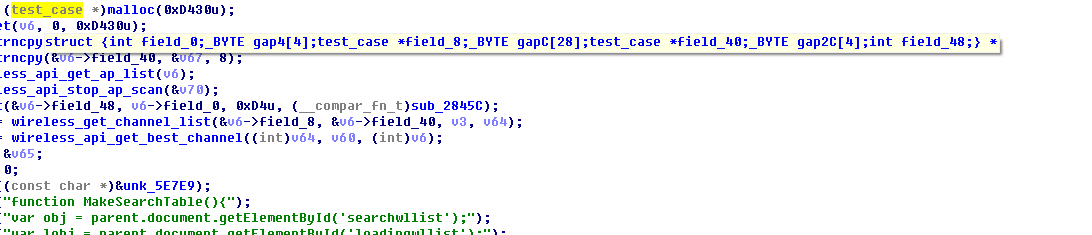




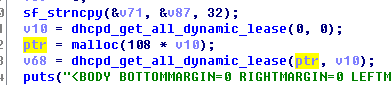
이전 와 동일합니다.

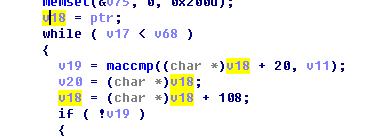
****

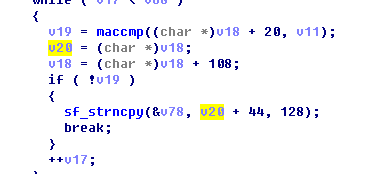
****

****

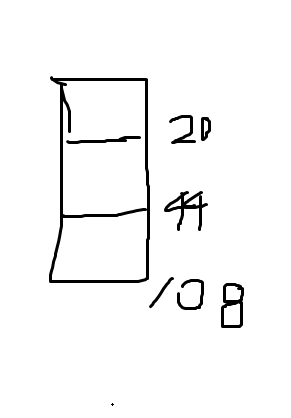
****

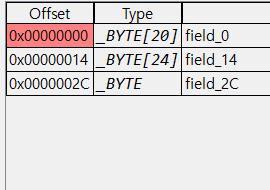
****

****

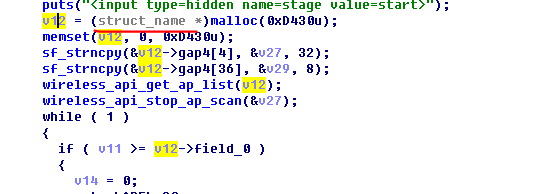
****

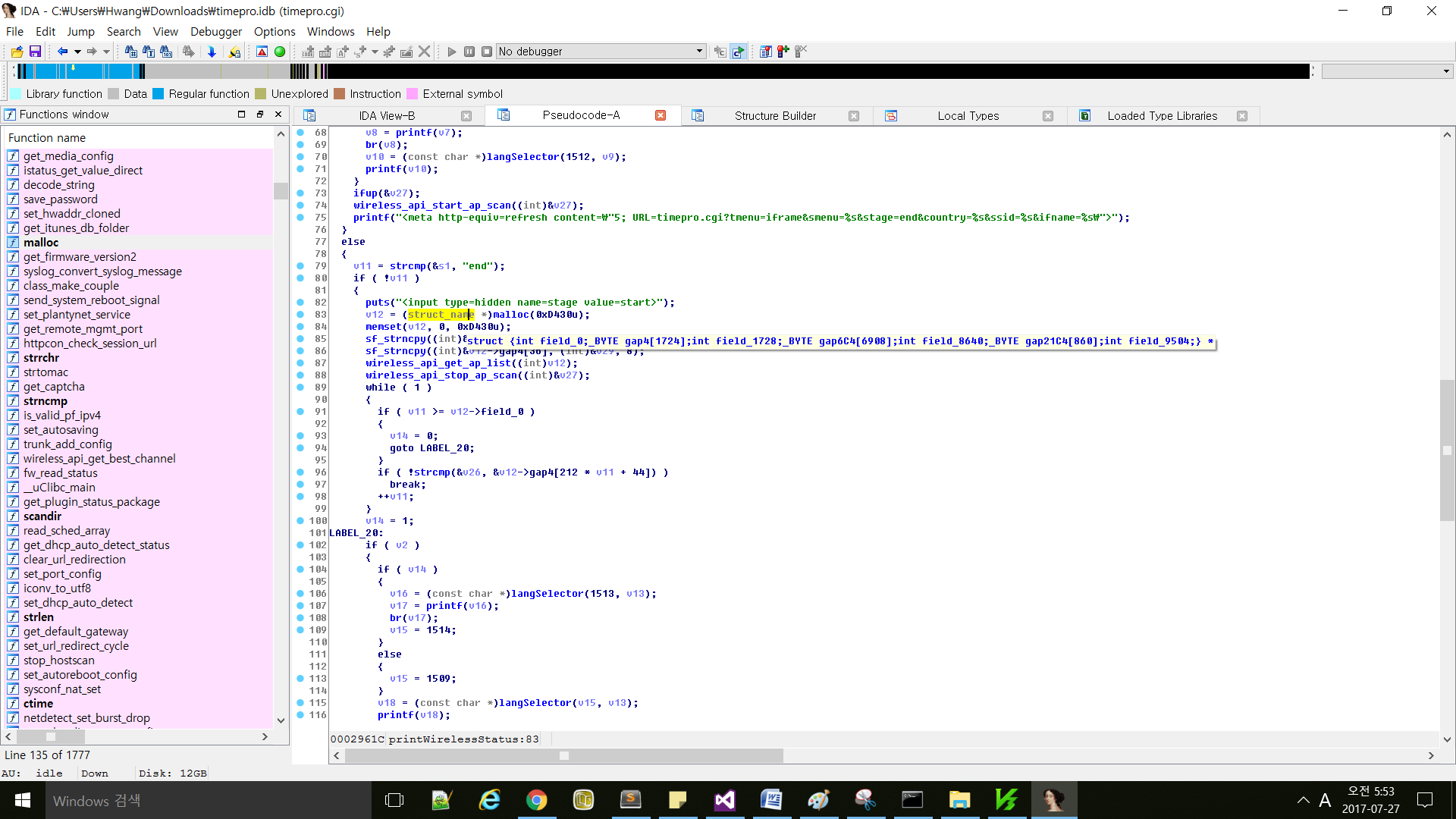
**Ptr 🡪 v18 🡪 v20**

****

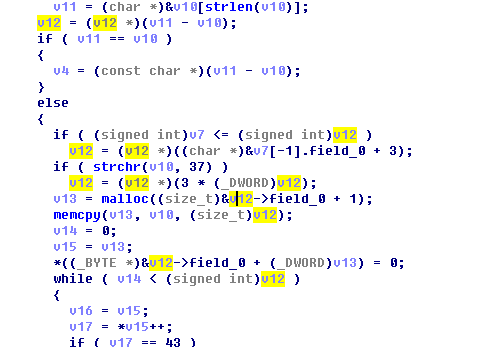
****

****

****

****

****

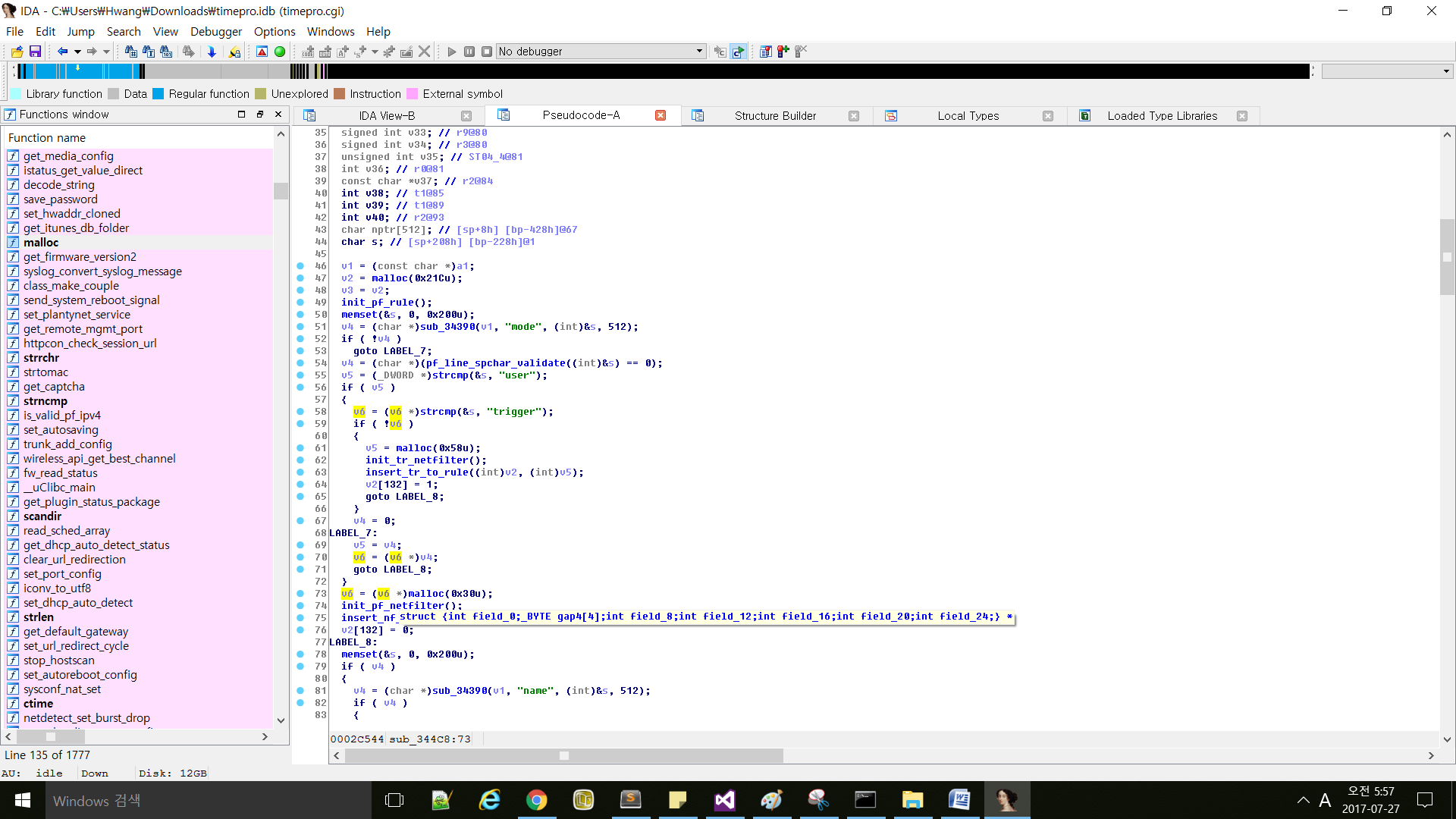
****

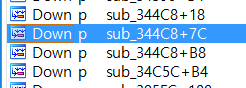
****

****

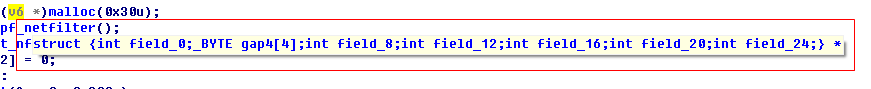
****

이전에 나왔던 구조체입니다.

****

****

****

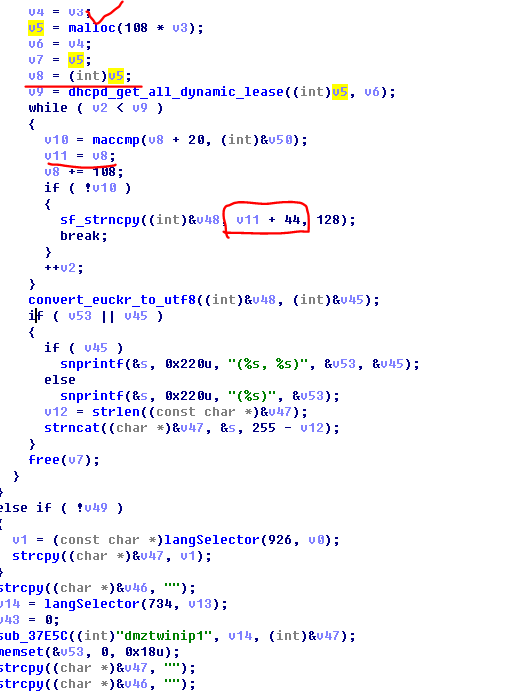
****

****

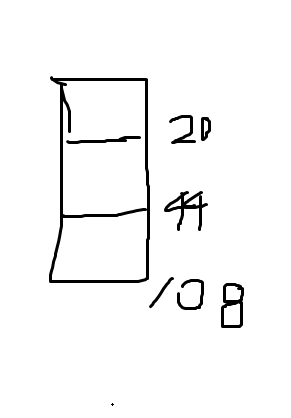
****

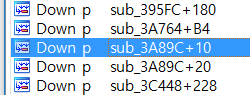
****

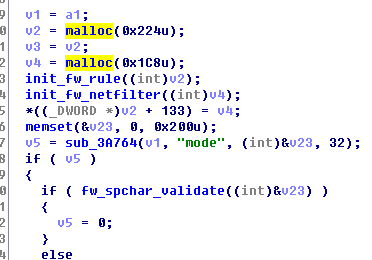
****

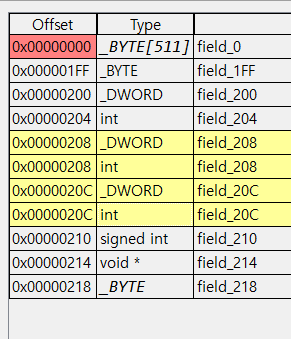
****

구조체가 ****와 같은 것으로 추정

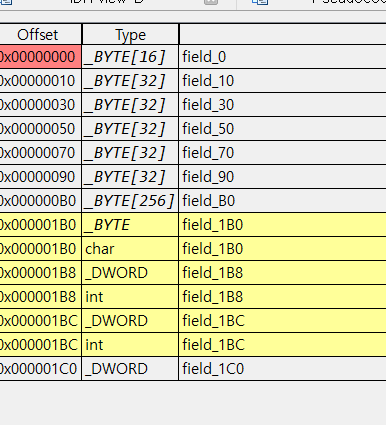


****

****

****

****

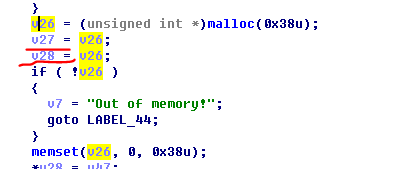
****

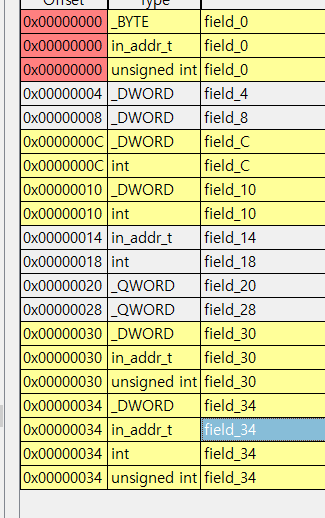
****

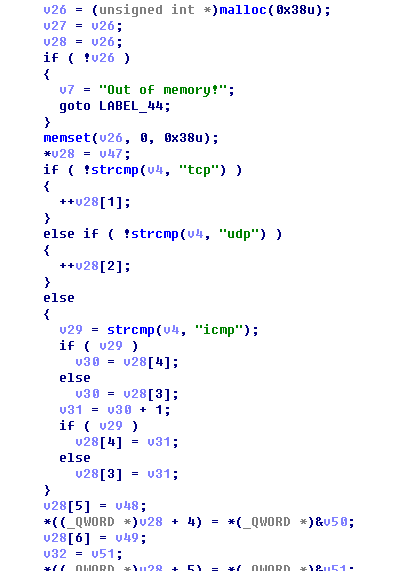
****

앞의  구조체와 동일합니다.

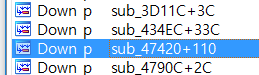
****

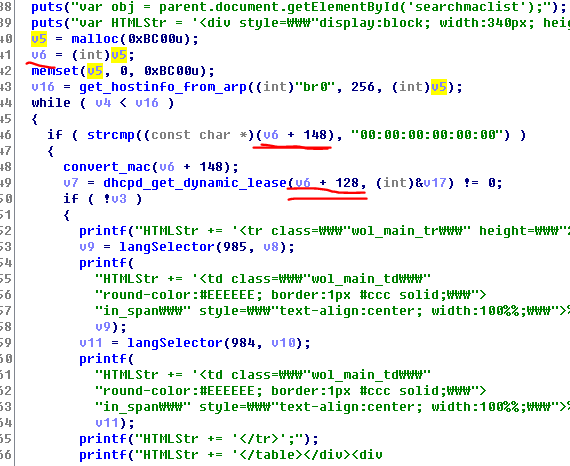
****

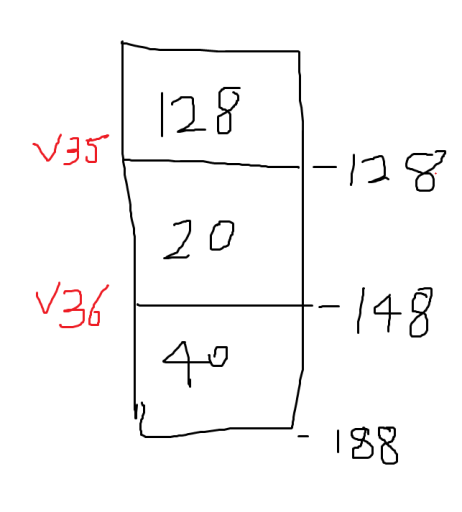
****

****

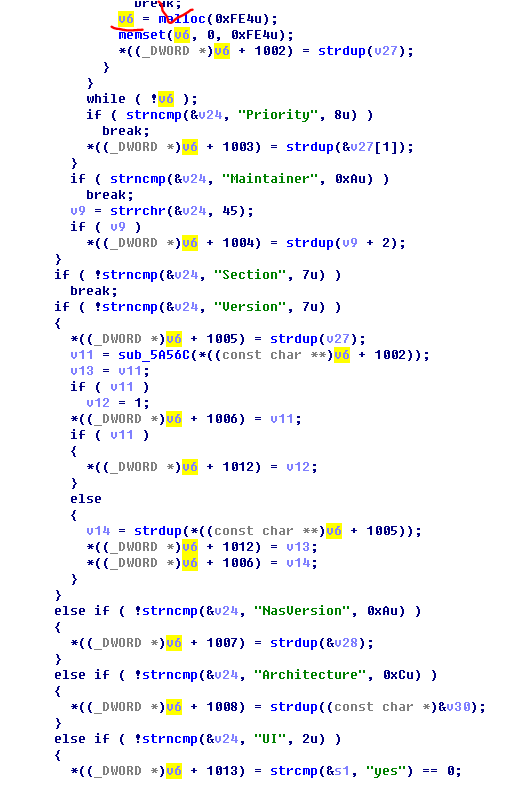
패킷 헤더 관련된 것으로 예상됩니다.

****

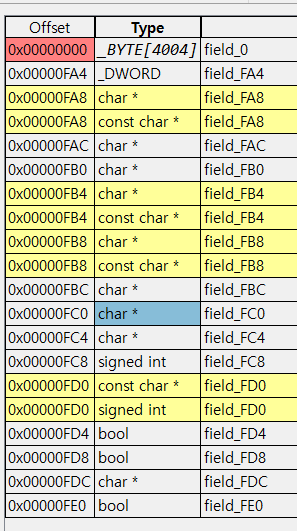
****

****이전에 나왔던 구조체와 동일합니다.





DWORD이므로 4바이트씩 증가합니다.



#pragma pack(push, 1)

struct CHANGE\_MY\_NAME // sub\_14830+1d0 //sub\_28ff4+144

{

DWORD field\_0;

DWORD field\_4;

BYTE field\_8[32];

BYTE field\_28[8];

BYTE field\_30[168];

DWORD field\_D8;

};

struct CHANGE\_MY\_NAME // sub\_1bcf0+310

{

\_BYTE field\_0[148];

char field\_94;

};

struct CHANGE\_MY\_NAME // sub\_2dfb4+14c

{

\_BYTE field\_0[20];

\_BYTE field\_14[24];

CHANGE\_MY\_NAME field\_2C;

};

struct CHANGE\_MY\_NAME // sub\_31434+1e8

{

\_BYTE field\_0[8];

\_BYTE field\_8[32];

\_BYTE field\_28;

};

struct CHANGE\_MY\_NAME // sub\_344c8+18

{

\_BYTE field\_0[4];

\_BYTE field\_4[512];

\_BYTE field\_204;

\_BYTE gap\_205[11];

\_DWORD field\_210;

};

struct CHANGE\_MY\_NAME // sub\_395fc+180

{

\_BYTE field\_0[20];

\_BYTE field\_14[24];

CHANGE\_MY\_NAME field\_2C;

};

struct CHANGE\_MY\_NAME // sub\_3a89c+10

{

\_BYTE field\_0[511];

\_BYTE field\_1FF;

\_DWORD field\_200;

int field\_204;

int field\_208;

int field\_20c;

signed int field\_210;

void \*field\_214;

\_BYTE field\_218;

};

struct CHANGE\_MY\_NAME // sub\_3a89c+20

{

\_BYTE field\_0[16];

\_BYTE field\_10[32];

\_BYTE field\_30[32];

\_BYTE field\_50[32];

\_BYTE field\_70[32];

\_BYTE field\_90[32];

\_BYTE field\_B0[256];

\_BYTE filed\_1b0;

int filed\_1b8;

int filed\_1bc;

\_DWORD filed\_1c0;

};

struct CHANGE\_MY\_NAME // sub\_434ec+33c // sub\_495dc+bc

{

\_BYTE field\_0[128];

\_BYTE filed\_80[20];

\_BYTE filed\_94;

};

struct CHANGE\_MY\_NAME // sub\_47420+110

{

\_QWORD filed\_0;

\_\_int64 field\_8;

\_\_int64 field\_10;

\_\_int64 field\_18;

\_\_int64 field\_20;

\_\_int64 field\_28;

\_\_int64 field\_30;

\_\_int64 field\_38;

\_\_int64 field\_40;

\_\_int64 field\_48;

\_\_int64 field\_50;

\_\_int64 field\_58;

\_\_int64 field\_60;

\_\_int64 field\_68;

\_\_int64 field\_70;

};

struct CHANGE\_MY\_NAME // sub\_4790c+2c

{

\_BYTE field\_0[10];

\_BYTE field\_A[10];

\_BYTE field\_14;

};

플러그인을 사용하여 구조체가 아님을 한 번 더 정확히 하고자 하였습니다.

플러그인을 통해 이전에 나왔는지 확신을 가질 수 있었습니다.

플러그인에 한계점이 있었기에 최대한 검수를 거치려고 노력했습니다.