너도 나도 다같이 리버싱!!!

IDA 분석 정보를 공유합시다!

oroi

Why?

- Ø 더럽게 많은 악성코드 !!!
- Ø 더럽게 어려운 바이너리 !!!
- Ø 혼자 못해먹겠다 싶을 때 !!!

Why?

- Ø 분석하다가 퇴근하고 싶은데 !!!
- Ø 같은 팀이 다 퇴근해서 인수 인계 안될 때 !!!
- Ø 나도 퇴근 좀 해보자 !!!

Concept

분석가 김씨

IDA Pro

IDB

I
D
B

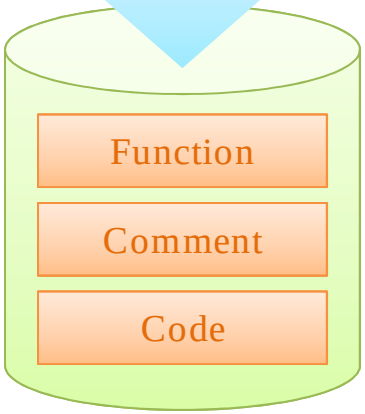
분석가 조씨

- ü 파일 주고 가라고 !!!
- ü 버전 안 맞아 !!!
- ü IDB 파일 너무 커!!!

분석가 김씨

IDA Pro

IDB



분석가 조씨

- ü 필요한 함수만 ^-^
- ü 버전은 암거나 ^-^
- ü 업데이트만 해줘 ^-^

IDA PRO???

```
00000F30  3B C7 8B 1D 80 11 00 01  89 7D FC 74 3A FF 35 80  ;?....??:  5..?.?
00000F40  4D 01 01 50 FF 15 7C 11  00 01 8D 45 D0 50 FF 35  M..P  .|....E?  5
00000F50  6C 4D 01 01 89 75 FC FF  D3 FF 35 6C 4D 01 01 FF  lM..뎦??5lM..   5
00000F60  15 78 11 00 01 FF 35 7C  4D 01 01 FF 15 74 11 00  .x...  5|M..  .t.
00000F70  01 89 3D 7C 4D 01 01 39  3D 48 4D 01 01 8B 35 70  .?|M..9=HM..?p.t.
00000F80  11 00 01 57 57 57 74 52  6A 66 FF 35 48 4A 01 01  ...WWWtRjf  5HJ..
00000F90  FF 15 6C 11 00 01 50 A3  6C 4D 01 01 FF 15 A4 10    .l...P즘M..  .?
00000FA0  00 01 39 3D A0 4D 01 01  A3 80 4D 01 01 0F 84 3D  ..9=좟..?M...? .?
00000FB0  01 00 00 6A EC FF 35 6C  4D 01 01 FF 15 68 11 00  ...j?5lM..  .h..?
00000FC0  01 0D 00 00 50 00 50 6A  EC FF 35 6C 4D 01 01 FF  ....P.Pj?5lM..  ?
00000FD0  15 64 11 00 01 E9 16 01  00 00 6A 65 FF 35 48 4A  .d...?..je  5HJ?
```

What the fuck!!!

무야는 이야기 그만!!!

```
.text:01009768 E8 4B ?? FF FF
.text:0100976D ?? ?8
.text:0100976F 6A E8 98 00 01
.text:01009774 E8 AB EA FF FF
.text:01009779 33 DB
.text:0100977B 89 5D E4
.text:0100977E 89 5D ??
.text:01009781 8? 45 98
.text:01009784 5?
.text:01009785 FF 15 4C 11 00 01
.text:0100978B C7 45 FC FE FF FF FF
.text:01009792 C7 45 FC 01 00 00 00
.text:01009799 64 A1 18 00 00 00
.text:0100979F 8B 70 04
.text:010097A2 BF 50 4A 05 01
```

```
call    __security_init_cookie
push    58h
push    offset dword_10098E0
call    __SEH_prolog4
xor     ebx, ebx
mov     [ebp-1Ch], ebx
mov     [ebp-4], ebx
lea     eax, [ebp-68h]
push    eax             ; lpStartupInfo
call    ds:__imp__GetStartupInfoA@4 ; GetStartupInfoA(x)
mov     dword ptr [ebp-4], 0FFFFFFFEh
mov     dword ptr [ebp-4], 1
mov     eax, large fs:18h
mov     esi, [eax+4]
mov     edi, offset __native_startup_lock
```

IDA PRO Plugins

CodeShare

분석가 김씨

IDA Pro

IDA Python

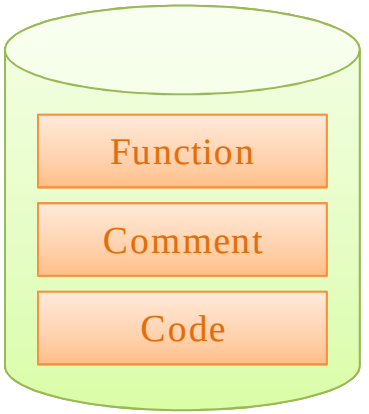
IDB

[Ctrl+4]This function : DB -> IDB
[Ctrl+5]This function : IDB -> DB
[Ctrl+6]This function : IDB(raw) -> DB
[Ctrl+7]ALL function : DB -> IDB
[Ctrl+8]ALL function : IDB -> DB
[Ctrl+9]ALL function : IDB(raw) -> DB

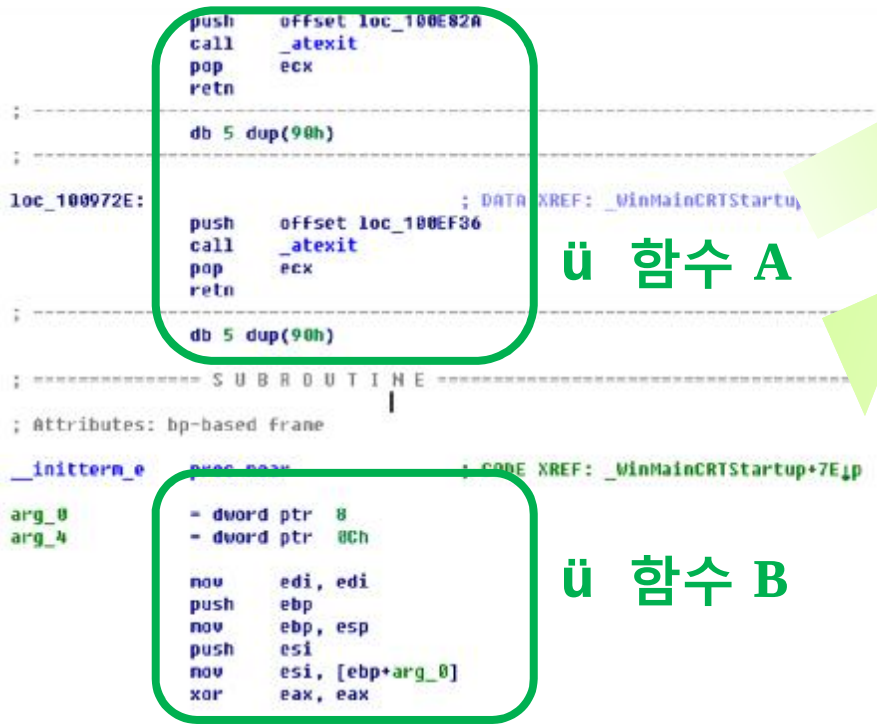
- ü Alt + F7 : Script Load
- ü CodeShare.py
  - GET or SET Reverse Information

RCEHUB

- ü GET.PHP : 분석 정보 추출
- ü SET.PHP : 분석 정보 저장
- ü MOD.PHP : WEB 작업용!



[Ctrl+4]This function : DB -> IDB



ü 함수 A

ü 함수 B

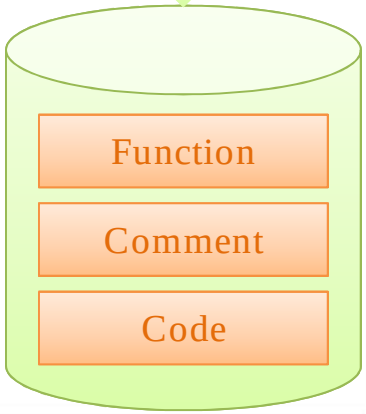
ü 마우스 포인터가 클릭한 위치의 함수 한 개에 대한 MD5 추출

ü Function MD5

ü Function Name

ü Comment

ü Offset



[Ctrl+5]This function : IDB -> DB

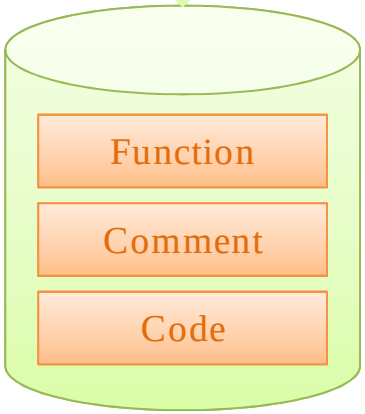
```
                push    offset loc_100E82A
                call    _atexit
                pop     ecx
                retn
; ---------------------------------------------------------------------------
                db 5 dup(90h)
; ---------------------------------------------------------------------------

loc_100972E:                            ; DATA XREF: _WinMainCRTStartu
                push    offset loc_100EF36
                call    _atexit
                pop     ecx
                retn
; ---------------------------------------------------------------------------
                db 5 dup(90h)
; ---------------------------------------------------------------------------

; ============== S U B R O U T I N E =======================================

; Attributes: bp-based frame

__initterm_e    proc near               ; CODE XREF: _WinMainCRTStartup+7E↓p

arg_0           = dword ptr  8
arg_4           = dword ptr  0Ch

                mov     edi, edi
                push    ebp
                mov     ebp, esp
                push    esi
                mov     esi, [ebp+arg_0]
                xor     eax, eax
```

ü 함수 A

ü 함수 B

ü 마우스 포인터가 클릭한 위치의 함수 한 개에 대한 MD5, 이름, 주석 정보를 추출

ü Function MD5
ü Function Name
ü Comment
ü Offset



[Ctrl+6]This function : IDB(raw) -> DB

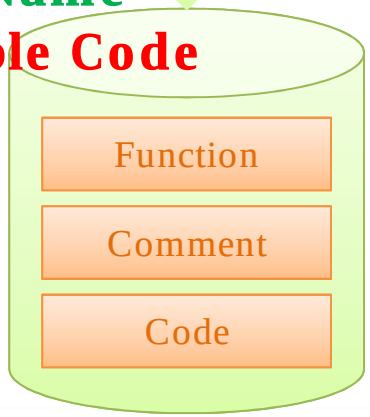
```
                push    offset loc_100E82A
                call    _atexit
                pop     ecx
                retn
; ---------------------------------------------------------------------------
                db 5 dup(90h)
; ---------------------------------------------------------------------------

loc_100972E:                            ; DATA XREF: _WinMainCRTStartu
                push    offset loc_100EF36
                call    _atexit
                pop     ecx
                retn
; ---------------------------------------------------------------------------
                db 5 dup(90h)
; ============== S U B R O U T I N E =======================================

; Attributes: bp-based frame

__initterm_e    proc near               ; CODE XREF: _WinMainCRTStartup+7E↓p

arg_0           = dword ptr  8
arg_4           = dword ptr  0Ch

                mov     edi, edi
                push    ebp
                mov     ebp, esp
                push    esi
                mov     esi, [ebp+arg_0]
                xor     eax, eax
```

ü 함수 A

ü 함수 B

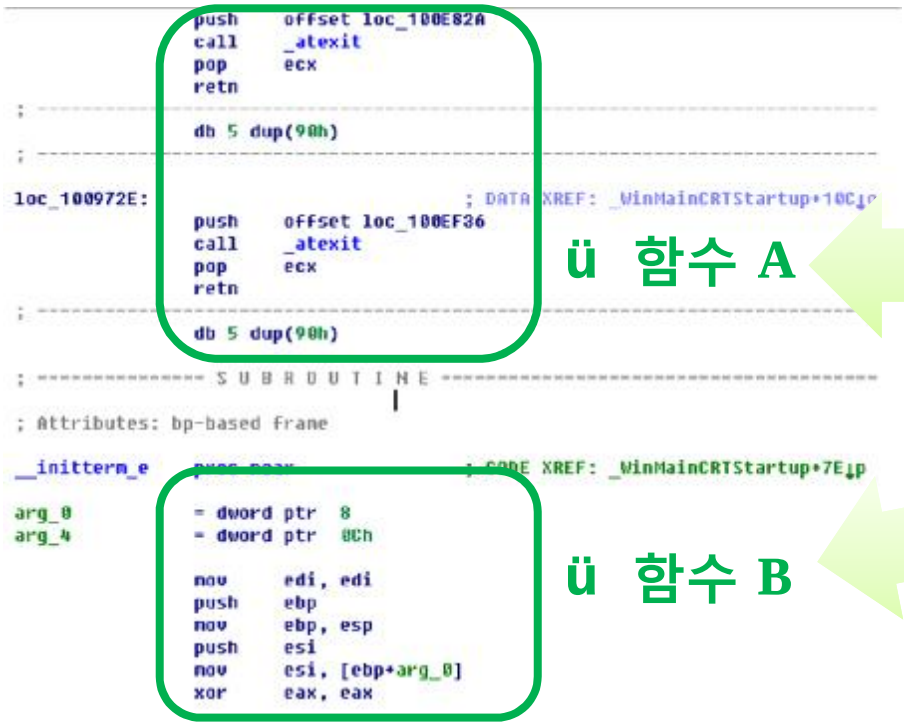
ü 마우스 포인터가 클릭한 위치의 함수 한 개에 대한 MD5, 이름, 디스어셈블 코드, 주석 정보를 추출

ü Function MD5
ü Function Name
ü Disassemble Code
ü Comment
ü Offset



CodeShare

[Ctrl+7]ALL function : DB -> IDB
[Ctrl+8]ALL function : IDB -> DB
[Ctrl+9]ALL function : IDB(raw) -> DB

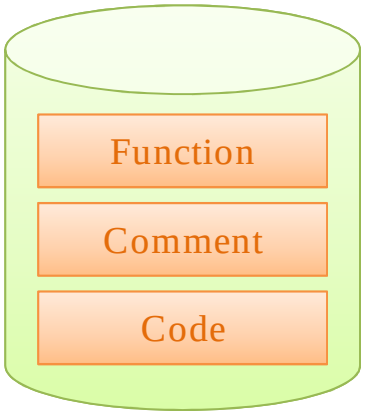


ü 함수 A

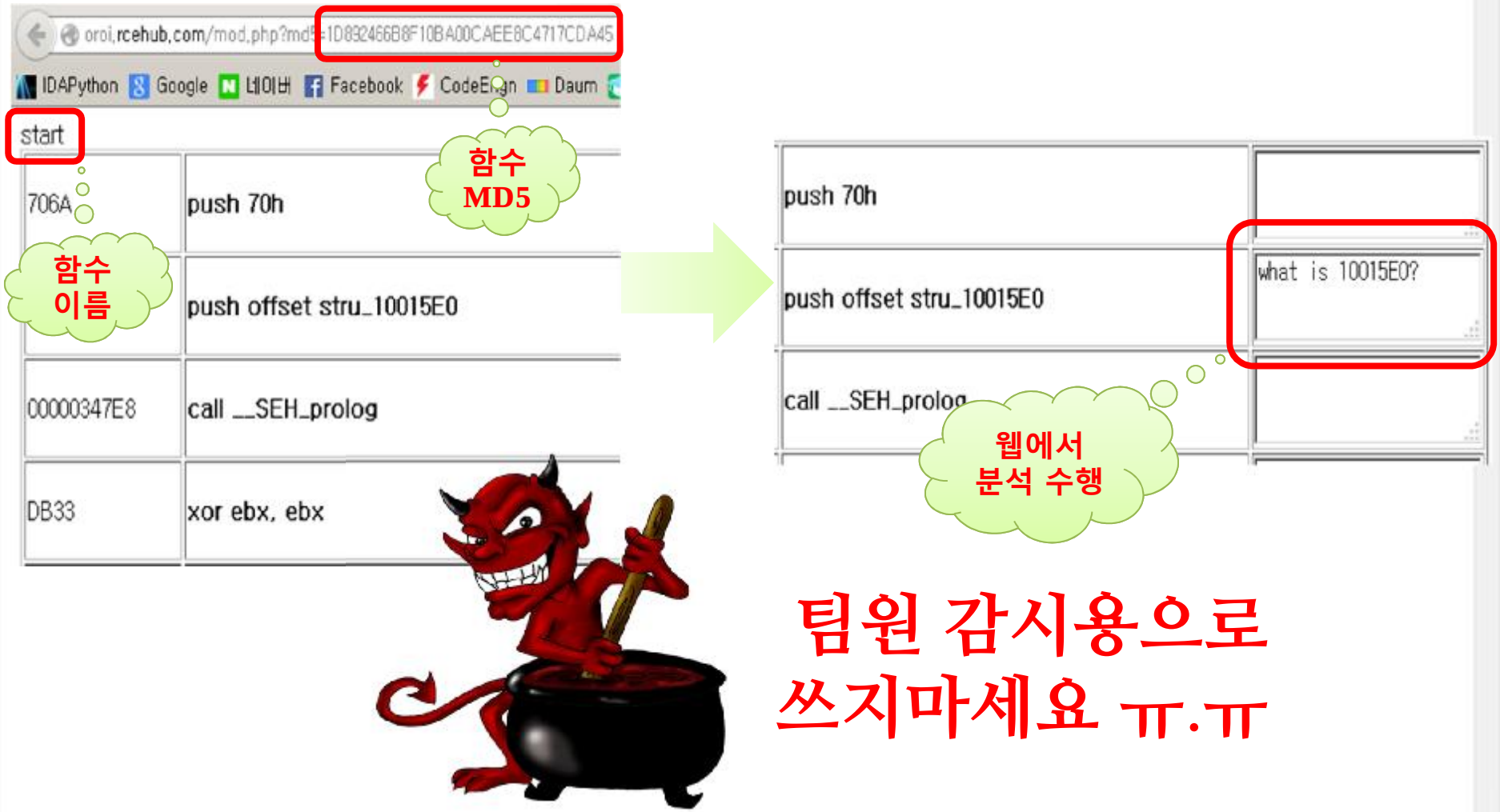
ü 함수 B

ü Function MD5
ü Function Name
ü Disassemble Code
ü Comment
ü Offset

ü Function MD5
ü Function Name
ü Disassemble Code
ü Comment
ü Offset

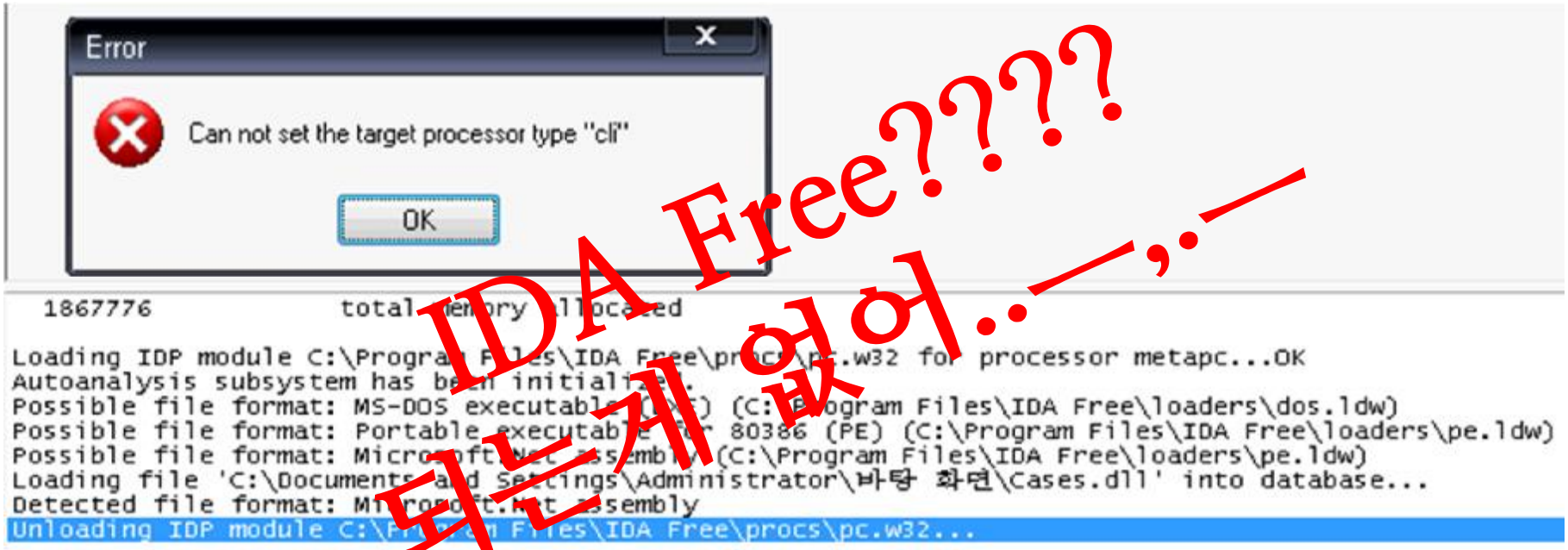


RAW ???


oroi.rcehub.com/mod.php?md5=1D892466B8F10BA00CAEE8C4717CDA45
IDAPython
Google
네이버
Facebook
CodeEngn
Daum
start
706A
push 70h
함수
MD5
함수
이름
push offset stru_10015E0
00000347E8
call __SEH_prolog
DB33
xor ebx, ebx
push 70h
push offset stru_10015E0
what is 10015E0?
call __SEH_prolog
웹에서
분석 수행
팀원 감시용으로
쓰지마세요 ㅠ.ㅠ


내 컴퓨터
codeshow...
휴지통
FileZilla Client
IDA Pro (64-bit)
Mozilla Firefox
heidisql
01.bmp
Notepad++
calc.exe
02.bmp
Wireshark
IDA Pro (32-bit)
시작
오전 2:44

IDA Pro 5.0 이상



IDA Free???? 뭐는게 없어..—,.—

Q & A