2nd CodeEngn Seminar

Immunity Debugger 활용 & Plugin 제작

유리바다(seaofglass@korea.com)

Code Engn

www.CodeEngn.com

차 례

- Episode Ⅰ
  - 격돌!
    Immunity Debugger vs Cheat Engine

- Episode Ⅱ
  - OEP를 찾아서

- Episode Ⅲ
  - 내 사랑 Plugin !

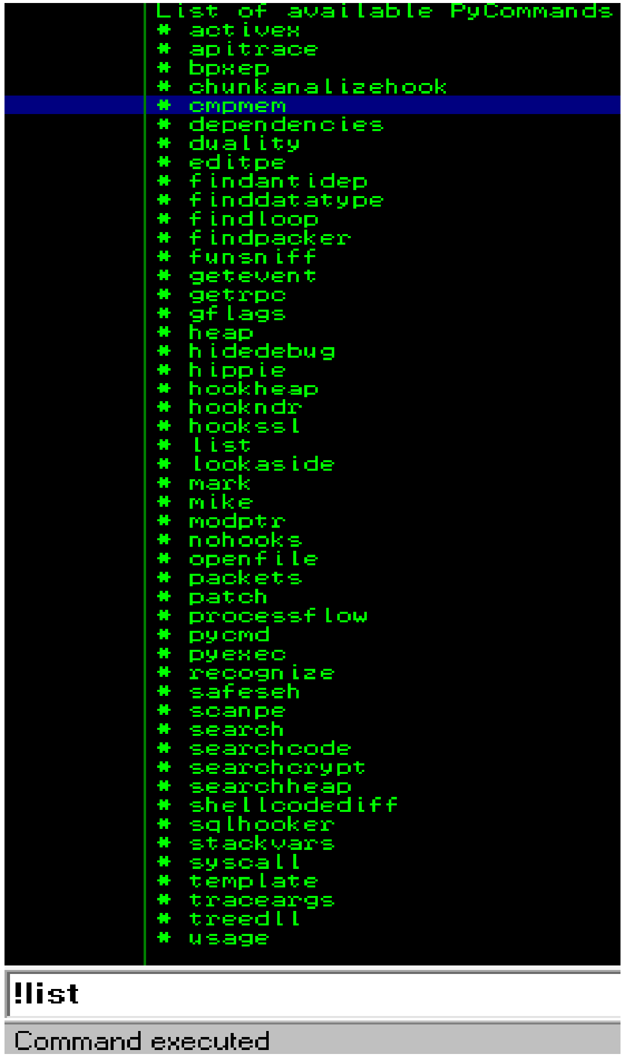
PyCommand

기본형식

!command

예) !list

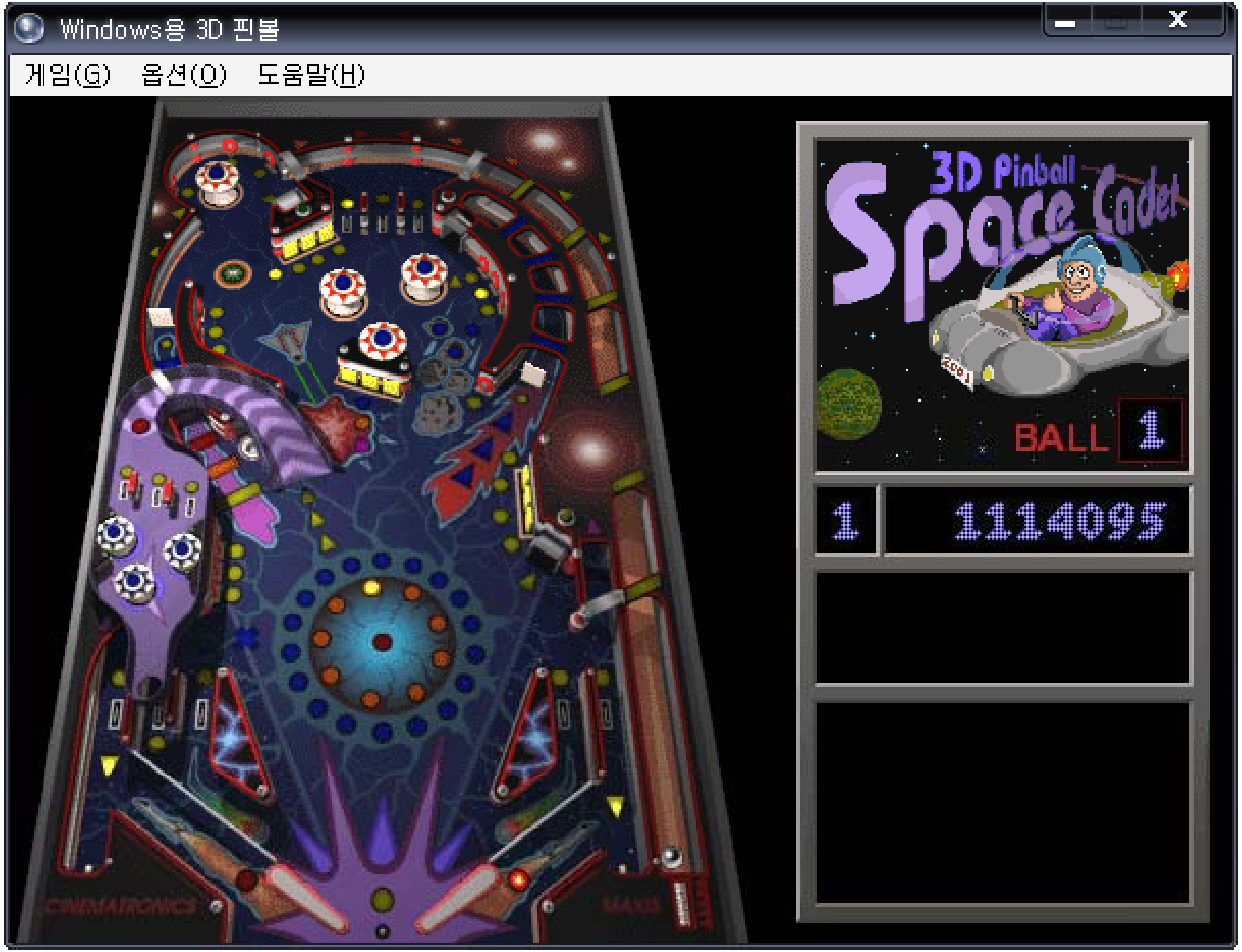
- 목록 보기



```
List of available PyCommands
* activex
* apitrace
* bpxep
* chunkanalizehook
* cmpmem
* dependencies
* duality
* editpe
* findantidep
* finddatatype
* findloop
* findpacker
* funsniff
* getevent
* getrpc
* gflags
* heap
* hidedebug
* hippie
* hookheap
* hookndr
* hookssl
* list
* lookaside
* mark
* mike
* modptr
* nohooks
* openfile
* packets
* patch
* processflow
* pycmd
* pyexec
* recognize
* safeseh
* scanpe
* search
* searchcode
* searchcrypt
* searchheap
* shellcodediff
* sqlhooker
* stackvars
* syscall
* template
* traceargs
* treedll
* usage
```

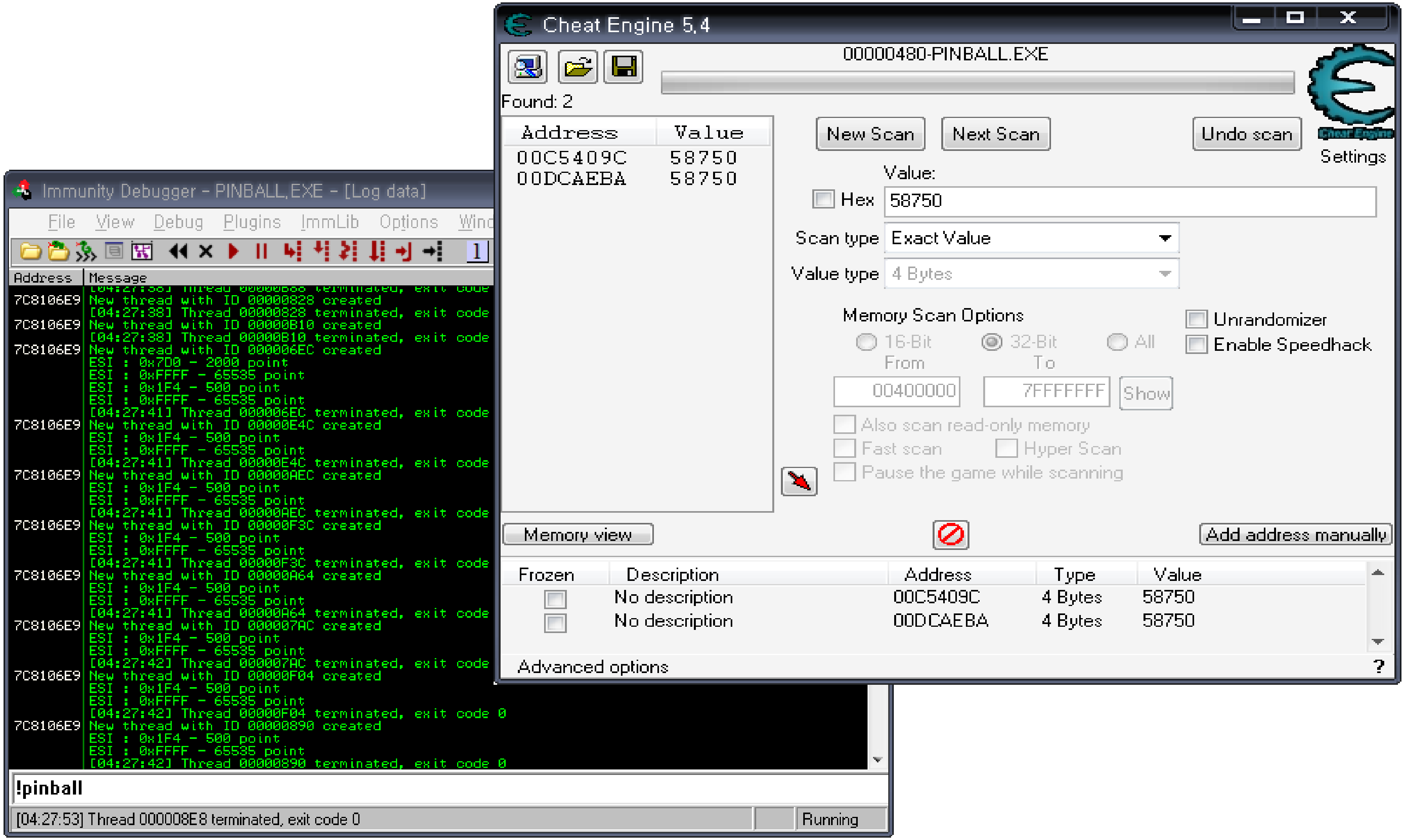
```
!list
Command executed
```

!pinball


Windows용 3D 핀볼
게임(G)
옵션(O)
도움말(H)
3D Pinball
Space Cadet
BALL 1
1
1114095
CINEMATRONICS
MAXIS

시연

Think!



```
Address   Message
7C8106E9  New thread with ID 00000828 created
          [04:27:38] Thread 00000828 terminated, exit code
7C8106E9  New thread with ID 00000B10 created
          [04:27:38] Thread 00000B10 terminated, exit code
7C8106E9  New thread with ID 000006EC created
          ESI : 0x7D0 - 2000 point
          ESI : 0xFFFF - 65535 point
          ESI : 0x1F4 - 500 point
          ESI : 0xFFFF - 65535 point
          [04:27:41] Thread 000006EC terminated, exit code
7C8106E9  New thread with ID 00000E4C created
          ESI : 0x1F4 - 500 point
          ESI : 0xFFFF - 65535 point
          [04:27:41] Thread 00000E4C terminated, exit code
7C8106E9  New thread with ID 00000AEC created
          ESI : 0x1F4 - 500 point
          ESI : 0xFFFF - 65535 point
          [04:27:41] Thread 00000AEC terminated, exit code
7C8106E9  New thread with ID 00000F3C created
          ESI : 0x1F4 - 500 point
          ESI : 0xFFFF - 65535 point
          [04:27:41] Thread 00000F3C terminated, exit code
7C8106E9  New thread with ID 00000A64 created
          ESI : 0x1F4 - 500 point
          ESI : 0xFFFF - 65535 point
          [04:27:41] Thread 00000A64 terminated, exit code
7C8106E9  New thread with ID 000007AC created
          ESI : 0x1F4 - 500 point
          ESI : 0xFFFF - 65535 point
          [04:27:42] Thread 000007AC terminated, exit code
7C8106E9  New thread with ID 00000F04 created
          ESI : 0x1F4 - 500 point
          ESI : 0xFFFF - 65535 point
          [04:27:42] Thread 00000F04 terminated, exit code 0
7C8106E9  New thread with ID 00000890 created
          ESI : 0x1F4 - 500 point
          ESI : 0xFFFF - 65535 point
          [04:27:42] Thread 00000890 terminated, exit code 0
```

```
!pinball
```

```
[04:27:53] Thread 000008E8 terminated, exit code 0    Running
```

Found: 2

```
Address    Value
00C5409C   58750
00DCAEBA   58750
```

Value:
□ Hex 58750

Scan type: Exact Value

Value type: 4 Bytes

Memory Scan Options

○ 16-Bit ● 32-Bit ○ All

From: 00400000 To: 7FFFFFFF Show

□ Also scan read-only memory
□ Fast scan □ Hyper Scan
□ Pause the game while scanning

□ Unrandomizer
□ Enable Speedhack

Frozen	Description	Address	Type	Value
□	No description	00C5409C	4 Bytes	58750
□	No description	00DCAEBA	4 Bytes	58750

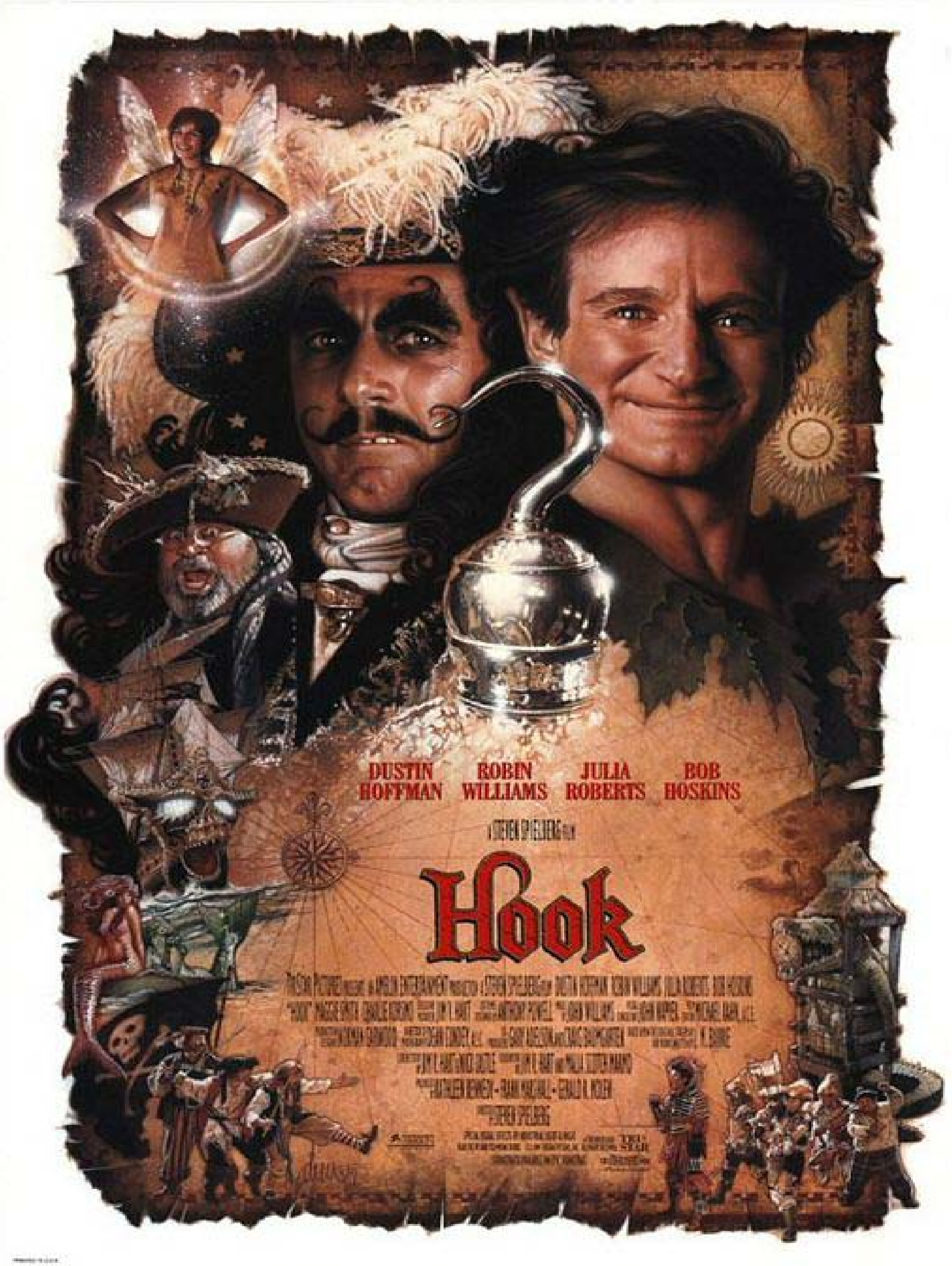
Pinball with HOOK?!

```
import immlib
from immlib import LogBpHook

class pinball_hooks(LogBpHook):
def __init__(self):
        LogBpHook.__init__(self)

def run(self, regs):
        imm = immlib.Debugger()
        imm.Run()

def main(args):
    imm = immlib.Debugger()
    bp_address = 0x0101757C
    logbp_hook = pinball_hooks()
    logbp_hook.add("pinball_game", bp_address)
```



immlib.py

- Log(“msg”)
  - Log 윈도우에 메시지를 남김 (Alt + L)

- updateLog()
  - Log 윈도우 업데이트

- setStatusBar(“msg”)
  - 상태창에 메시지 설정

- clearStatusBar()
  - 상태창에 설정된 메시지 지움

immlib.py

- stepIn()   # F7
- stepOver()   # F8
- Run()   # F9

- runTillRet()   # Ctrl+F9

- setBreakpoint(0xbadc0ded)
- deleteBreakpoint(0xbadc0ded)

immlib.py

- writeMemory(self, address, buf)
  - 메모리 지정한 주소에 데이터 쓰기

- readMemory(self, address, size)
  - 메모리로 부터 지정한 크기의 데이터 읽기

- isvmWare()
  - 현재 디버거가 vmware에서 작동 여부 확인

immlib.py

- isAnalysed(regs['EIP'])
  - 코드가 분석되어져 있는가?
- analyseCode(regs['EIP'])
  - 코드 분석 수행
- openTextFile(path="")
  - MDI창으로 텍스트 파일을 읽어온다.

immlib.py

- regs=imm.getRegs()

  imm.Log("OEP : 0x%08X " % regs['EIP'])

- setReg("ESP", 0xFFFFFFFF)

- getDebuggedName()
  - 디버깅되고 있는 process module 이름 얻기

immlib.py

- getDebuggedPid()
  - 디버깅되고 있는 프로세스 아이디 얻기
- isAdmin()
  - 디버깅이 운영자 권한으로 실행되는가 여부
- ps()
  - 현재 활성화 된 프로세스 리스트 얻기

immlib.py

- getAllThreads()
  - 모든 프로세스의 thread 리스트 얻기
- callStack()
  - Back Trace를 리스트 형으로 얻어옴
- markBegin(), markEnd()
  - 시작 마크, 종료 마크 (시간 값)

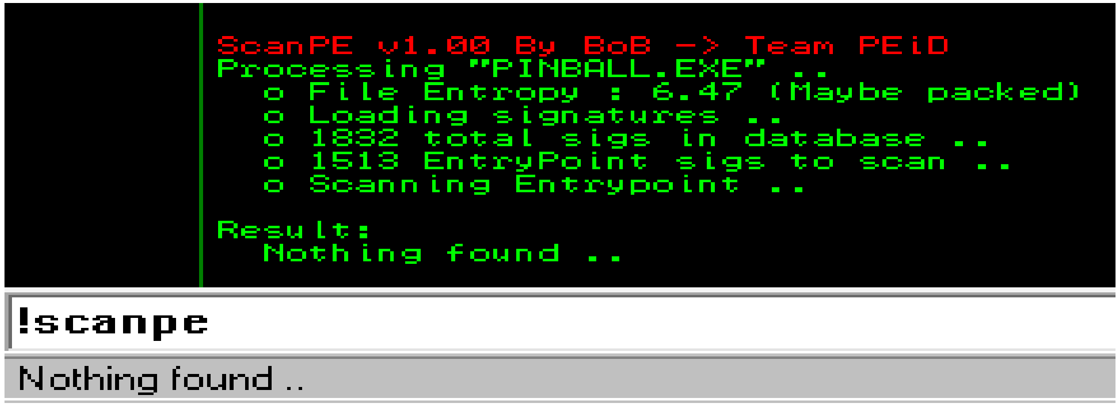
immlib.py

- inputBox(“title”)
  - 입력 창 생성

- comboBox(“title”, “[list1, list2]”)
  - 콤보 박스 생성

Episode Ⅱ

넌 누구냐?

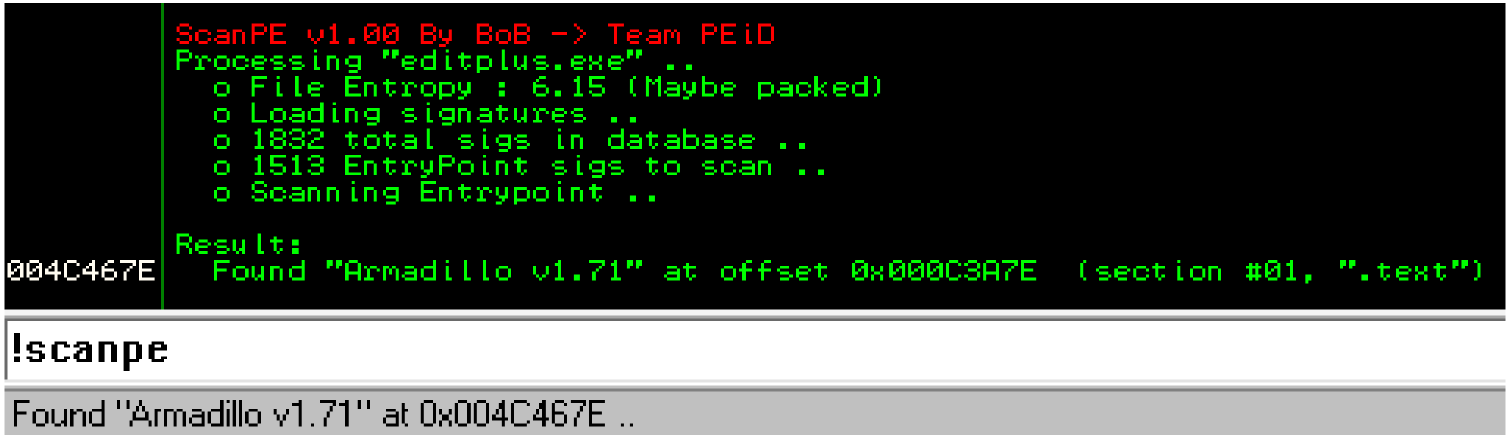


```
ScanPE v1.00 By BoB -> Team PEiD
Processing "PINBALL.EXE" ..
   o File Entropy : 6.47 (Maybe packed)
   o Loading signatures ..
   o 1832 total sigs in database ..
   o 1513 EntryPoint sigs to scan ..
   o Scanning Entrypoint ..

Result:
   Nothing found ..
```

```
!scanpe
```

Nothing found ..



```
          ScanPE v1.00 By BoB -> Team PEiD
          Processing "editplus.exe" ..
             o File Entropy : 6.15 (Maybe packed)
             o Loading signatures ..
             o 1832 total sigs in database ..
             o 1513 EntryPoint sigs to scan ..
             o Scanning Entrypoint ..

          Result:
004C467E     Found "Armadillo v1.71" at offset 0x000C3A7E  (section #01, ".text")
```

```
!scanpe
```

Found "Armadillo v1.71" at 0x004C467E ..

Unpacker OEP 찾기!

- 예제 : FSG 2.0
  - OP Code를 이용하여 원하는 위치 찾기
  - BreakPoint 걸기
  - 디버거를 실행하여 BP 위치 도달
  - BreakPoint 해제
  - StepOver()로 OEP 도달하기

주소 찾기

```
#code = "JMP DWORD PTR DS:[EBX+C]”
opcode = "₩xFF₩x63₩x0C”

res = imm.Search(opcode)
```

Search( ) 함수

- 입력 : OP Code
- 출력 : 찾은 주소 (리스트 형)

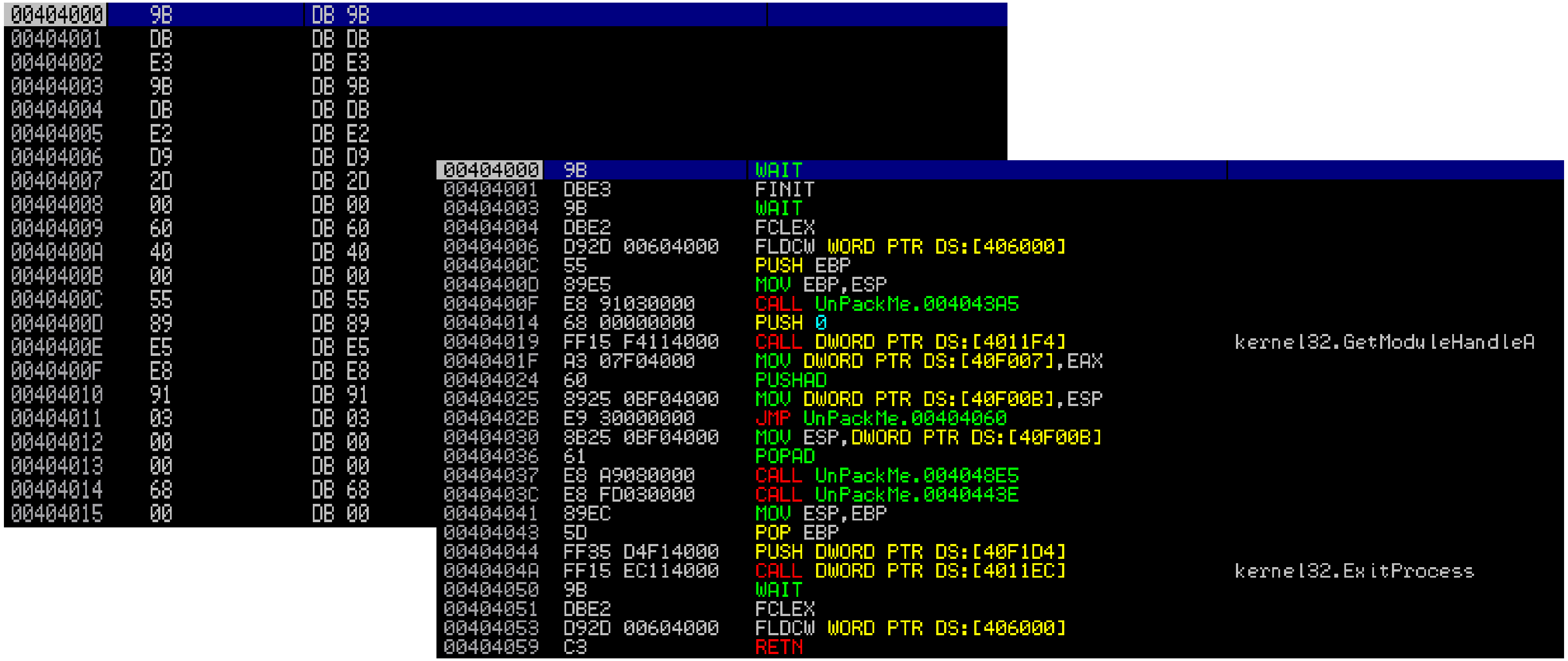
디버거 구동

1. 찾은 주소로 중단점 설정
2. 실행 후 중단점에서 정지
3. 중단점 해지

```
imm.setBreakpoint(res[0])
imm.Run(1)
imm.deleteBreakpoint(res[0])
```

코드 분석 여부 파악

imm.isAnalysed(regs['EIP'])
imm.analyseCode(regs['EIP'])

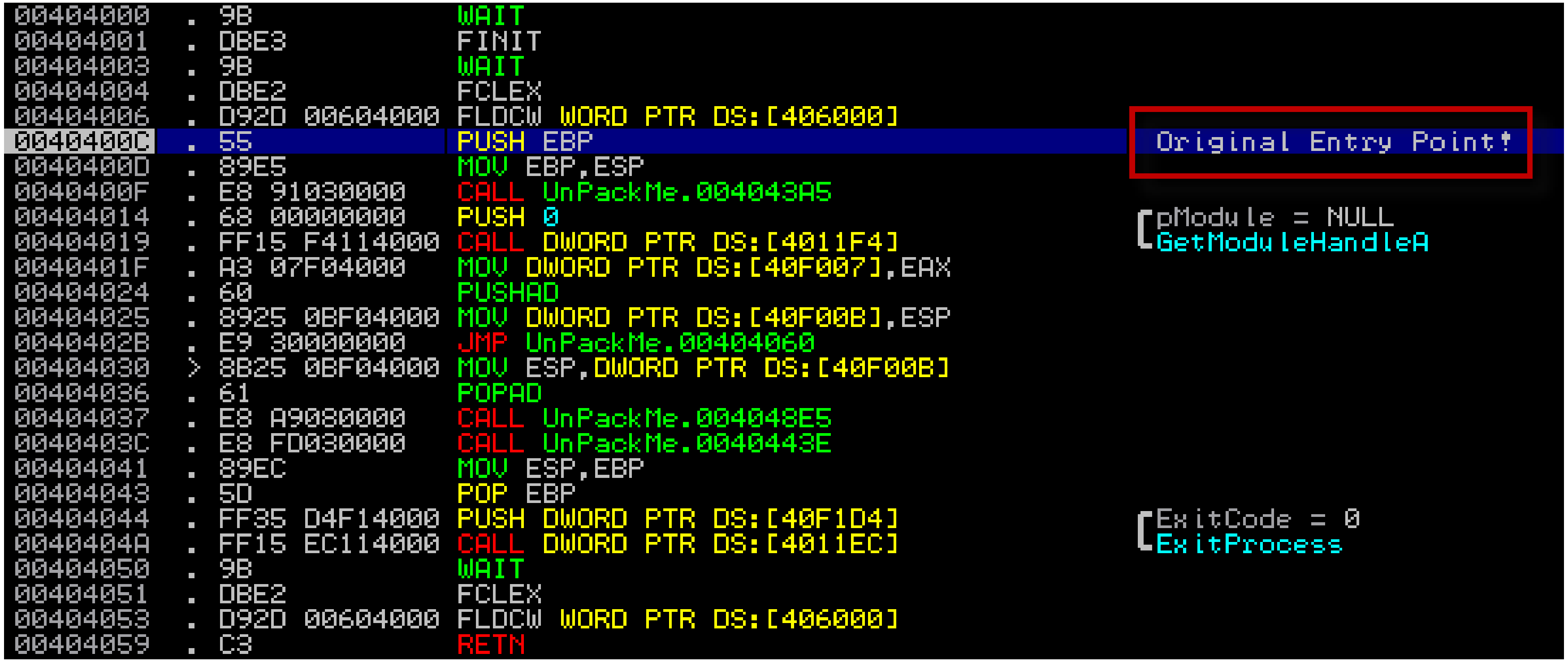


```
00404000   9B      DB 9B
00404001   DB      DB DB
00404002   E3      DB E3
00404003   9B      DB 9B
00404004   DB      DB DB
00404005   E2      DB E2
00404006   D9      DB D9
00404007   2D      DB 2D
00404008   00      DB 00
00404009   60      DB 60
0040400A   40      DB 40
0040400B   00      DB 00
0040400C   55      DB 55
0040400D   89      DB 89
0040400E   E5      DB E5
0040400F   E8      DB E8
00404010   91      DB 91
00404011   03      DB 03
00404012   00      DB 00
00404013   00      DB 00
00404014   68      DB 68
00404015   00      DB 00
```

```
00404000   9B              WAIT
00404001   DBE3            FINIT
00404003   9B              WAIT
00404004   DBE2            FCLEX
00404006   D92D 00604000   FLDCW WORD PTR DS:[406000]
0040400C   55              PUSH EBP
0040400D   89E5            MOV EBP,ESP
0040400F   E8 91030000     CALL UnPackMe.004043A5
00404014   68 00000000     PUSH 0
00404019   FF15 F4114000   CALL DWORD PTR DS:[4011F4]                 kernel32.GetModuleHandleA
0040401F   A3 07F04000     MOV DWORD PTR DS:[40F007],EAX
00404024   60              PUSHAD
00404025   8925 0BF04000   MOV DWORD PTR DS:[40F00B],ESP
0040402B   E9 30000000     JMP UnPackMe.00404060
00404030   8B25 0BF04000   MOV ESP,DWORD PTR DS:[40F00B]
00404036   61              POPAD
00404037   E8 A9080000     CALL UnPackMe.004048E5
0040403C   E8 FD030000     CALL UnPackMe.0040443E
00404041   89EC            MOV ESP,EBP
00404043   5D              POP EBP
00404044   FF35 D4F14000   PUSH DWORD PTR DS:[40F1D4]
0040404A   FF15 EC114000   CALL DWORD PTR DS:[4011EC]                 kernel32.ExitProcess
00404050   9B              WAIT
00404051   DBE2            FCLEX
00404053   D92D 00604000   FLDCW WORD PTR DS:[406000]
00404059   C3              RETN
```

OEP에 주석 달기

```
regs = imm.getRegs()
imm.setComment(regs['EIP'], “OEP!")
```



```
00404000  . 9B             WAIT
00404001  . DBE3           FINIT
00404003  . 9B             WAIT
00404004  . DBE2           FCLEX
00404006  . D92D 00604000  FLDCW WORD PTR DS:[406000]
0040400C  . 55             PUSH EBP                                        Original Entry Point!
0040400D  . 89E5           MOV EBP,ESP
0040400F  . E8 91030000    CALL UnPackMe.004043A5
00404014  . 68 00000000    PUSH 0                                         [pModule = NULL
00404019  . FF15 F4114000  CALL DWORD PTR DS:[4011F4]                     [GetModuleHandleA
0040401F  . A3 07F04000    MOV DWORD PTR DS:[40F007],EAX
00404024  . 60             PUSHAD
00404025  . 8925 0BF04000  MOV DWORD PTR DS:[40F00B],ESP
0040402B  . E9 30000000    JMP UnPackMe.00404060
00404030  > 8B25 0BF04000  MOV ESP,DWORD PTR DS:[40F00B]
00404036  . 61             POPAD
00404037  . E8 A9080000    CALL UnPackMe.004048E5
0040403C  . E8 FD030000    CALL UnPackMe.0040443E
00404041  . 89EC           MOV ESP,EBP
00404043  . 5D             POP EBP
00404044  . FF35 D4F14000  PUSH DWORD PTR DS:[40F1D4]                     [ExitCode = 0
0040404A  . FF15 EC114000  CALL DWORD PTR DS:[4011EC]                     [ExitProcess
00404050  . 9B             WAIT
00404051  . DBE2           FCLEX
00404053  . D92D 00604000  FLDCW WORD PTR DS:[406000]
00404059  . C3             RETN
```

Packer OEP 찾기 시연

- 예제 FSG 2.0

Episode III

plugin 제작

- PDK(Plugin Development Kit)를 통한 제작
- 작성 언어 : 델파이(Delphi)
- http://www.peid.info/BobSoft/Source/PDKforDelphi.zip (지원 라이브러리 및 샘플)

IMMDBG_Plugindata()

```
function IMMDBG_Plugindata(name: PChar):
  Integer; cdecl;
begin
  StrLCopy(name, PChar(PLUGIN_NAME), 32);
  // Name of plugin
  Result := PLUGIN_VERSION;
end;
```

IMMDBG_Plugininit()

```
function IMMDBG_Plugininit(ImmDbgVersion:
   Integer; hWndImmDbg: HWND; features:
   PULONG): Integer; cdecl;
begin

  g_hwndImmDbg := hWndImmDbg;
  Addtolist(0, 0, 'ImmunityDebugger Plugin');

  Result := 0;
end;
```

IMMDBG_Pluginmenu()

```
function IMMDBG_Pluginmenu(origin: Integer; pData: PChar; pItem:
    Pointer): Integer; cdecl;
begin
  case origin of
    PM_MAIN:
      begin
        // Plugin menu in main window
        StrCopy(pData, '0 &menu1, 1 &menu2,|2 &About...');
        Result := 1;
      end;
  else
    Result := 0; // Any other window
  end;
end;
```

IMMDBG_Pluginaction()

```
procedure IMMDBG_Pluginaction(origin: Integer; action: Integer; pItem: Pointer); cdecl;
var
  sExePath: string;
begin
  if (origin = PM_MAIN) then
  begin
    sExePath := GetExePath;
    case action of
      0: MessageBox(g_hwndImmDbg, PChar(MENU1), PChar(PLUGIN_NAME), MB_OK);
      1: MessageBox(g_hwndImmDbg, PChar(MENU2), PChar(PLUGIN_NAME), MB_OK);
      2: MessageBox(g_hwndImmDbg, PChar(ABOUT), PChar(PLUGIN_NAME), MB_OK);
    end;
  end;
end;
```

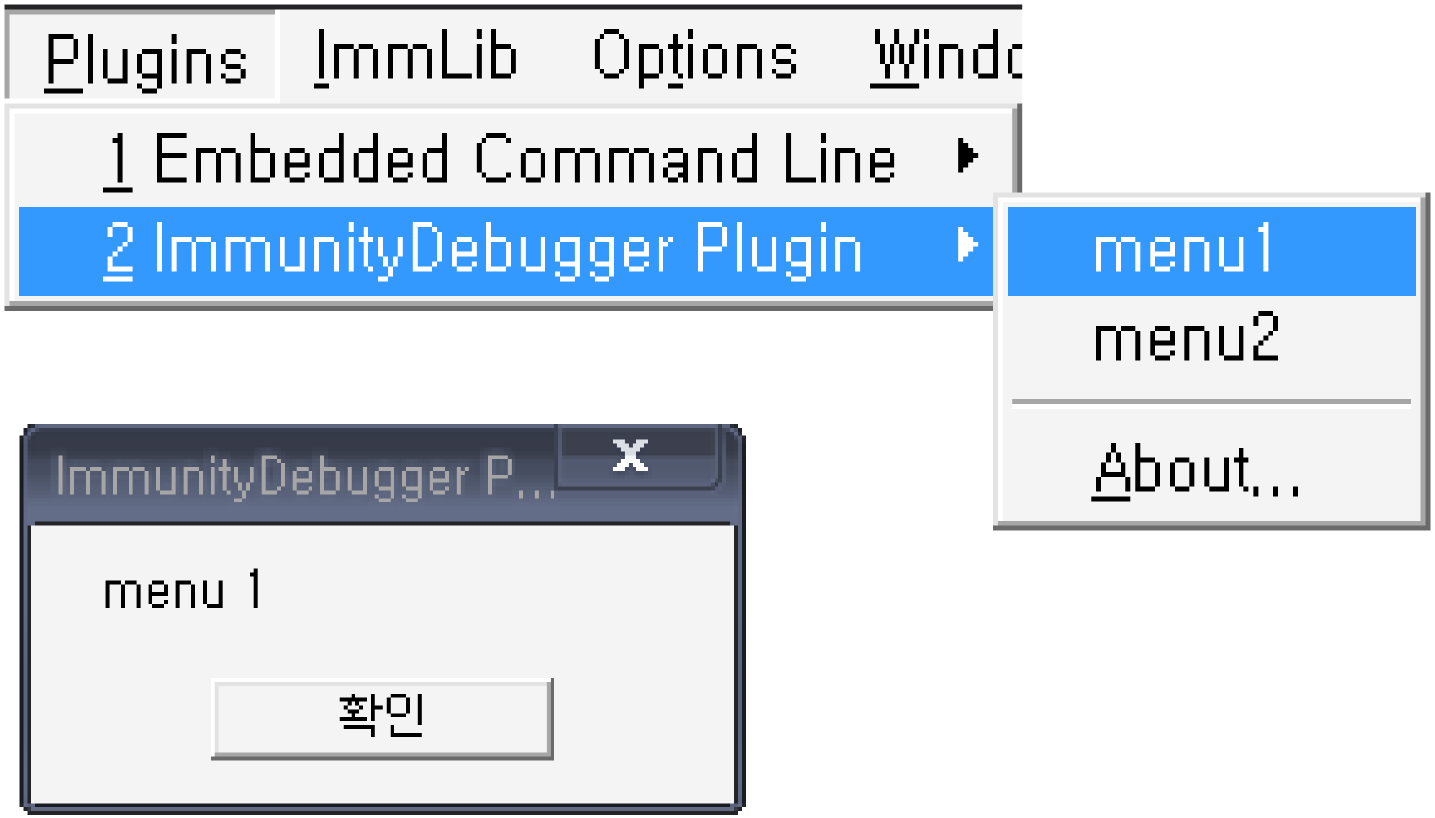
Plugin.pas

- PM_MAIN : 메인 윈도우 처리
- PM_DUMP : DUMP창 처리
- PM_THREADS : THREADS창 처리
- PM_BREAKPOINTS : BreakPoint 창 처리
- PM_RTRACE : Run Trace 창 처리
- PM_DISASM : CPU창 팝업 메뉴 처리
- PM_CPUREGS : CPU Register 처리

Plugin.pas

- TIMMDBG_Pluginmainloop()
- TIMMDBG_Pluginsaveudd()
- TIMMDBG_Pluginuddrecord()
- TIMMDBG_Pluginshortcut()
- TIMMDBG_Pluginreset()
- TIMMDBG_Pluginclose()
- TIMMDBG_Plugindestroy()

Sample plugin



menu 1

참고 사이트

- 이뮤니티 포럼
  - http://forum.immunityinc.com
- PDK for Delphi
  - http://www.peid.info/BobSoft/

Quiz

Reverse Engineering과 연관 있다고 생각되는 동물과 그 이유?

평가 – 공감성, 논리성

앞으로의 여정?

배우고자 하는 누군가를 위하여

학습 할 수 있는 토대를 만드는 것은

참으로 의미 있는 일이다!

2nd CodeEngn Seminar

감사합니다

Code Engn

www.CodeEngn.com