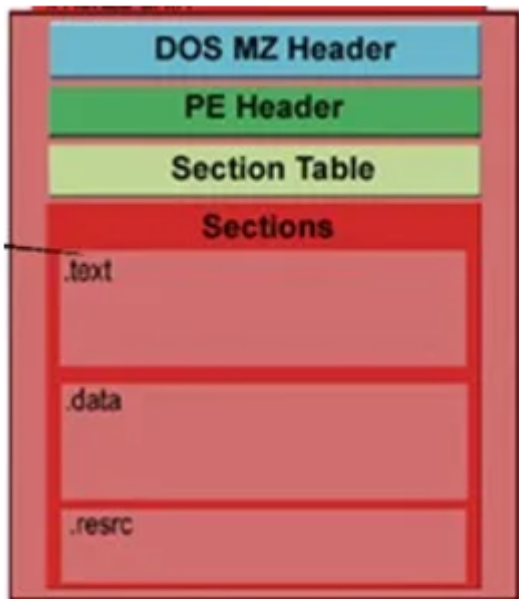


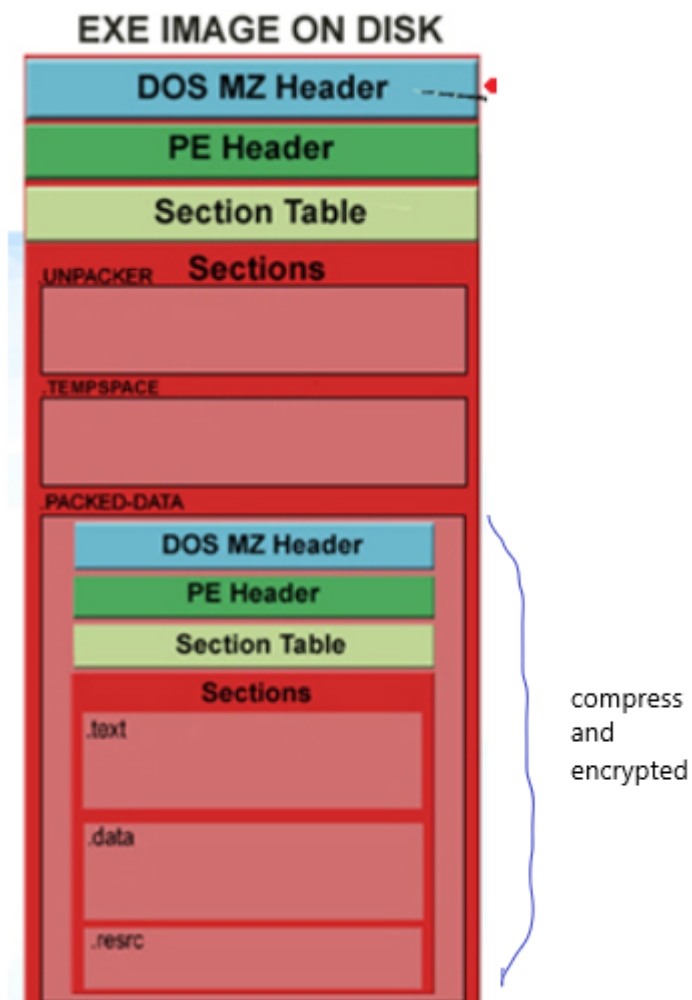
VCS_Báo cáo bài tập tuần 6 Reverse Engineering

0. Tổng quan packer

Cấu trúc file PE:

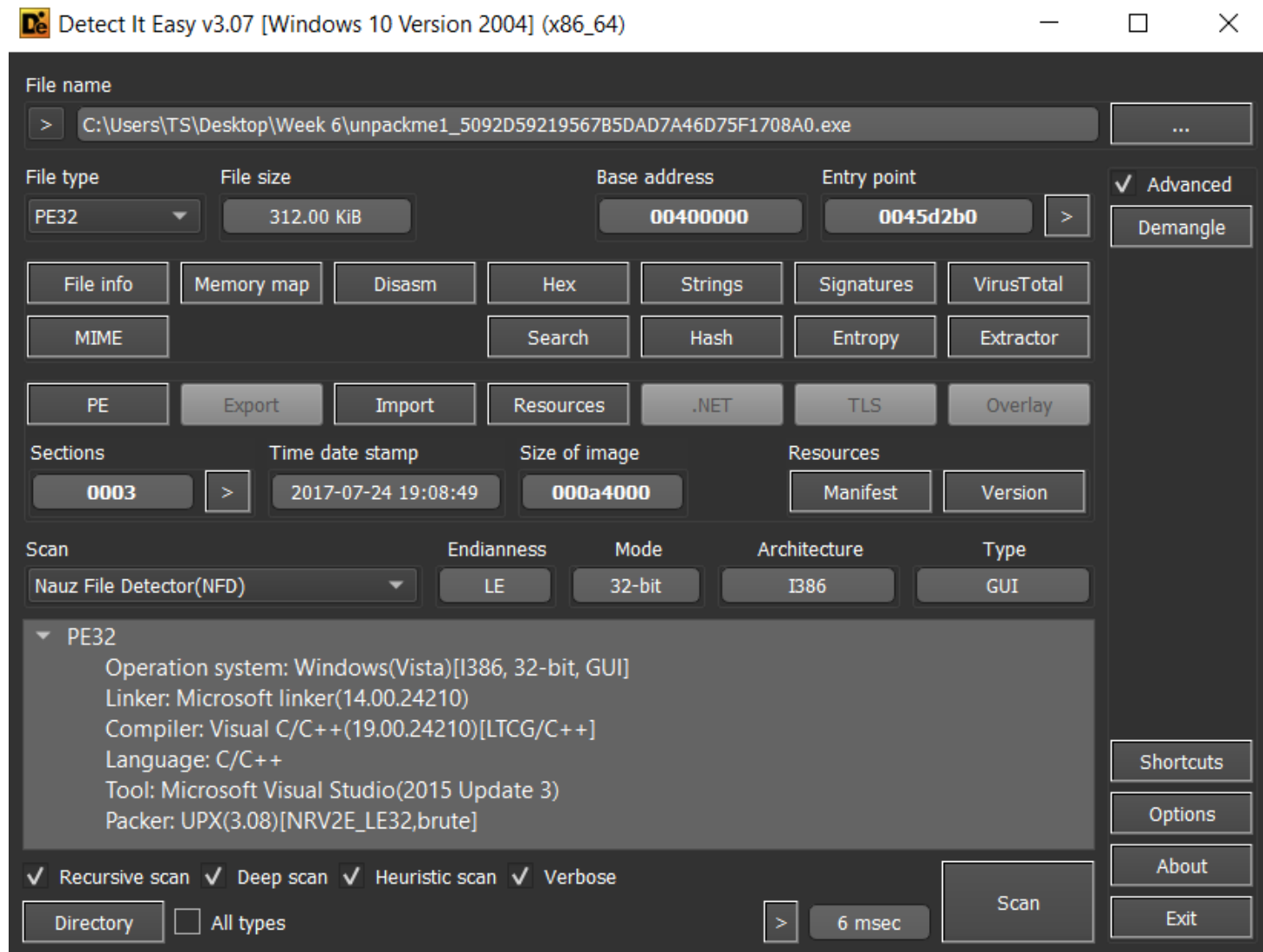


Cấu trúc file PE packed:



unpackme1_5092D59219567B5DAD7A46D75F1708A0.exe

Kiểm tra file bằng Detect It Easy cho thấy file được pack bằng UPX Packer:



UPX hoạt động theo các bước:

1. Lưu tất cả các trạng thái register với PUSHAD
2. Giải nén tất cả các phần trong bộ nhớ
3. Sửa IAT
4. Khôi phục trạng thái register bằng POPAD
5. Chuyển đến OEP và thực thi chương trình gốc.

Do vậy đặt breakpoint sau lệnh POPAD và dump file ra để unpack. Thực hiện trong x32dbg:

00401313	8B45 E0	mov eax,dword ptr ss:[ebp-20]
00401316	E8 3B070000	call unpackme1_5092d59219567b5dad7a46d75f
00401318	C3	ret
0040131C	E8 90030000	call unpackme1_5092d59219567b5dad7a46d75f
00401321	E9 8EFEFFFF	jmp unpackme1_5092d59219567b5dad7a46d75f
00401326	55	push ebp
00401327	8BEC	mov ebp,esp
00401329	6A 00	push 0
0040132B	FF15 24C04000	call dword ptr ds:[&SetUnhandledExceptionFilter]
00401331	FF75 08	push dword ptr ss:[ebp+8]
00401334	FF15 20C04000	call dword ptr ds:[&UnhandledExceptionFilter]
0040133A	68 090400C0	push C0000409
0040133F	FF15 28C04000	call dword ptr ds:[&GetCurrentProcess]
00401345	50	push eax
00401346	FF15 2CC04000	call dword ptr ds:[&TerminateProcess]
0040134C	5D	pop ebp
0040134D	C3	ret
0040134E	55	push ebp
0040134F	8BEC	mov ebp,esp
00401351	81FC 24030000	sub esp,324

Xóa dll bị lỗi, dump và fix dump bằng plugin scylla:

Scylla x86 v0.9.8

File Imports Trace Misc Help

Attach to an active process

0992 - unpackme1_5092D59219567B5DAD7A46D75F1708A0.exe - C:\Users\TS\Desktop\Wee ▾ Pick DLL

Imports

- comctl32.dll (1) FThunk: 0000C000
- kernel32.dll (64) FThunk: 0000C008
- user32.dll (5) FThunk: 0000C10C

Show Invalid Show Suspect Clear

IAT Info

OEP 0040131C IAT Autosearch

VA 0040C000 Get Imports

Size 00000128

Actions

Autotrace

Dump

Dump PE Rebuild

Fix Dump

Log

IAT Search Adv: IAT VA 0040C000 RVA 0000C000 Size 0x0128 (296)
IAT Search Nor: IAT VA 0040BFFC RVA 0000BFFC Size 0x0134 (308)
IAT parsing finished, found 70 valid APIs, missed 1 APIs
DIRECT IMPORTS - Found 0 possible direct imports with 0 unique APIs!
Dump success C:\Users\TS\Desktop\Week 6\unpackme1_5092D59219567B5DAD7A46D75F1708A0_dump.
Import Rebuild success C:\Users\TS\Desktop\Week 6\unpackme1_5092D59219567B5DAD7A46D75F1708A0

Imports: 70 Invalid: 0 Imagebase: 00400000 unpackme1 5092D5921

File unpack và chạy thành công:

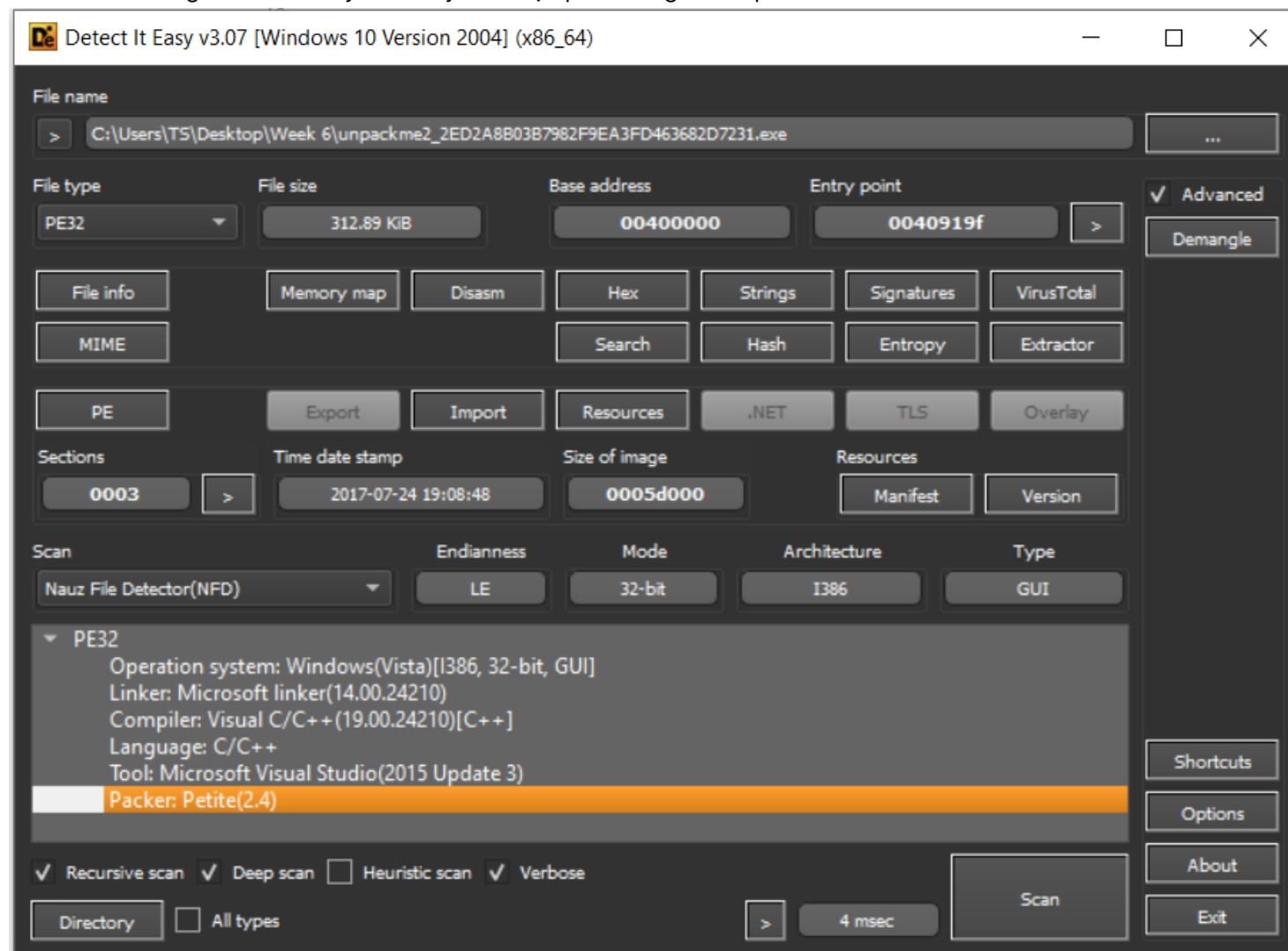
~~~ unpackme ~~~

Unpack me and write the solution

OK

unpackme2\_2ED2A8B03B7982F9EA3FD463682D7231.exe

Kiểm tra file bằng Detect It Easy cho thấy file được pack bằng Petite packer:



Debug file bằng x32dbg và f9 để đến EntryPoint. F7 qua và đặt hardware breakpoint ở địa chỉ ESP đang trỏ sau lệnh pushad:

|            |               |                                          |                |
|------------|---------------|------------------------------------------|----------------|
| → 0040919F | B8 00C04500   | mov eax,unpackme2_2ed2a8b03b7982f9ea3fd4 | EntryPoint     |
| 004091A4   | 60            | pushad                                   |                |
| → 004091A5 | 8DA8 0040FAFF | lea ebp,dword ptr ds:[eax-5C000]         |                |
|            | B2B91FFF      | push FF1FB9B2                            |                |
| 004091B0   | 6A 40         | push 40                                  |                |
| 004091B2   | 68 00300000   | push 3000                                |                |
| 004091B7   | 68 6F5F0000   | push 5F6F                                |                |
| 004091BC   | 6A 00         | push 0                                   |                |
| 004091BE   | FF90 16010000 | call dword ptr ds:[eax+116]              |                |
| 004091C4   | 894424 1C     | mov dword ptr ss:[esp+1C],eax            |                |
| 004091C8   | BB 57030000   | mov ebx,357                              |                |
| 004091CD   | 8DB5 B08E0000 | lea esi,dword ptr ss:[ebp+8EB0]          | esi:EntryPoint |
| 004091D3   | 8BF8          | mov edi,eax                              | edi:EntryPoint |
| 004091D5   | 50            | push eax                                 |                |

execute till return qua hàm virtual alloc và tìm được OEP 0x401308, dump bằng Scylla:

Log Breakpoints Memory Map Call Stack

00401308 E8 8A020000 call unpackme2\_2ed2a8b03b7982f9ea3fd46368  
 00401309 E9 8EFFFFFF jmp unpackme2\_2ed2a8b03b7982f9ea3fd46368  
 00401312 55 push ebp  
 00401313 8BEC mov ebp,esp  
 00401315 A1 38204100 mov eax,dword ptr ds:[412038]  
 0040131A 83E0 1F and eax,1F  
 0040131D 6A 20 push 20  
 0040131F 59 pop ecx  
 00401320 2BC8 sub ecx,eax  
 00401322 8B45 08 mov eax,dword ptr ss:[ebp+8]  
 00401325 D3C8 ror eax,cl  
 00401327 3305 38204100 xor eax,dword ptr ds:[412038]  
 0040132D 5D pop ebp  
 0040132E C3 ret  
 0040132F 55 push ebp  
 00401330 8BEC mov ebp,esp  
 00401332 8B45 08 mov eax,dword ptr ss:[ebp+8]  
 00401335 56 push esi  
 00401336 8B48 3C mov ecx,dword ptr ds:[eax+3C]  
 00401339 03C8 add ecx,eax  
 0040133B 0FB741 14 movzx eax,word ptr ds:[ecx+14]  
 0040133F 8D51 18 lea edx,dword ptr ds:[ecx+18]  
 00401342 03D0 add edx,eax  
 00401344 0FB741 06 movzx eax,word ptr ds:[ecx+6]  
 00401348 6BF0 28 imul esi,eax,28  
 0040134B 03F2 add esi,edx  
 0040134D 3BD6 cmp edx,esi  
 0040134F 74 19 je unpackme2\_2ed2a8b03b7982f9ea3fd463682  
 00401351 8B40 0C mov ecx,dword ptr ss:[ebp+C]  
 00401354 3B4A 0C cmp ecx,dword ptr ds:[edx+C]  
 00401357 72 0A jb unpackme2\_2ed2a8b03b7982f9ea3fd463682  
 00401359 8B42 08 mov eax,dword ptr ds:[edx+8]  
 0040135C 0342 0C add eax,dword ptr ds:[edx+C]  
 0040135F 3BC8 cmp ecx,eax  
 00401361 72 0C jb unpackme2\_2ed2a8b03b7982f9ea3fd463682

ea3fd463682d7231.00401597

b03b7982f9ea3fd463682d7231.exe:\$1308 #708

|       | Dump 3      | Dump 4      | Dump 5 | Watch 1           | [x=] Locals | Str |
|-------|-------------|-------------|--------|-------------------|-------------|-----|
|       | ASCII       |             |        |                   |             |     |
| 19 00 | BC 2B 6B 77 | 12 47 62 75 | ...    | Pý..%+kw.Gbu      |             |     |
| 19 00 | 58 FF 19 00 | 00 80 00 00 | ...    | ýýýýTý..xý        |             |     |
| 19 00 | D5 46 62 75 | FF FF FF FF | ...    | ..@.ý..0Fbuýýýý   |             |     |
| 00 00 | 00 80 00 00 | 80 FF 19 00 | ...    | ...               |             |     |
| 1F 00 | 00 00 00 00 | 00 80 00 00 | ...    | ..@.              |             |     |
| 32 00 | 10 FA 55 77 | DC FF 19 00 | ...    | )úUw.Ä2...úUúýý.. |             |     |
| 32 00 | 35 F3 48 95 | 00 00 00 00 | ...    | .zjw.Ä2.5ôH.....  |             |     |
| 32 00 | 00 00 00 00 | 00 00 00 00 | ...    | .....Ä2.....      |             |     |

Scylla x86 v0.9.8

File Imports Trace Misc Help

Attach to an active process

7588 - unpackme2\_2ED2A8B03B7982F9EA3FD463682D7231.exe - C:\Users\TS\Desktop\RE\R Pick DLL

Imports

- comctl32.dll (1) FThunk: 0000C000
- kernel32.dll (13) FThunk: 0000C008
- ? (2) FThunk: 0000C03C
- kernel32.dll (9) FThunk: 0000C044
- ? (1) FThunk: 0000C068
- kernel32.dll (2) FThunk: 0000C06C
- ? (1) FThunk: 0000C074
- kernel32.dll (2) FThunk: 0000C078
- ? (1) FThunk: 0000C080
- kernel32.dll (4) FThunk: 0000C084
- ? (2) FThunk: 0000C094
- kernel32.dll (1) FThunk: 0000C09C
- ? (2) FThunk: 0000C0A0

Show Invalid Show Suspect Clear

IAT Info

OEP 00401308 IAT Autosearch

VA 0040C000 Get Imports

Size 00000128

Actions

Autotrace

Dump

Dump PE Rebuild

Fix Dump

Log

IAT Search Adv: Found 71 (0x47) possible IAT entries.  
 IAT Search Adv: Possible IAT first 0040C000 last 0040C124 entry.  
 IAT Search Adv: IAT VA 0040C000 RVA 0000C000 Size 0x0128 (296)  
 IAT Search Nor: IAT VA 0040BFFC RVA 0000BFFC Size 0x0134 (308)  
 IAT parsing finished, found 55 valid APIs, missed 16 APIs  
 DIRECT IMPORTS - Found 0 possible direct imports with 0 unique APIs!

Imports: 71 Invalid: 16 Imagebase: 00400000 unpackme2\_2ED2A8B03

IAT bị hỏng nên file không chạy được nhưng có thể phân tích tĩnh:

Function name

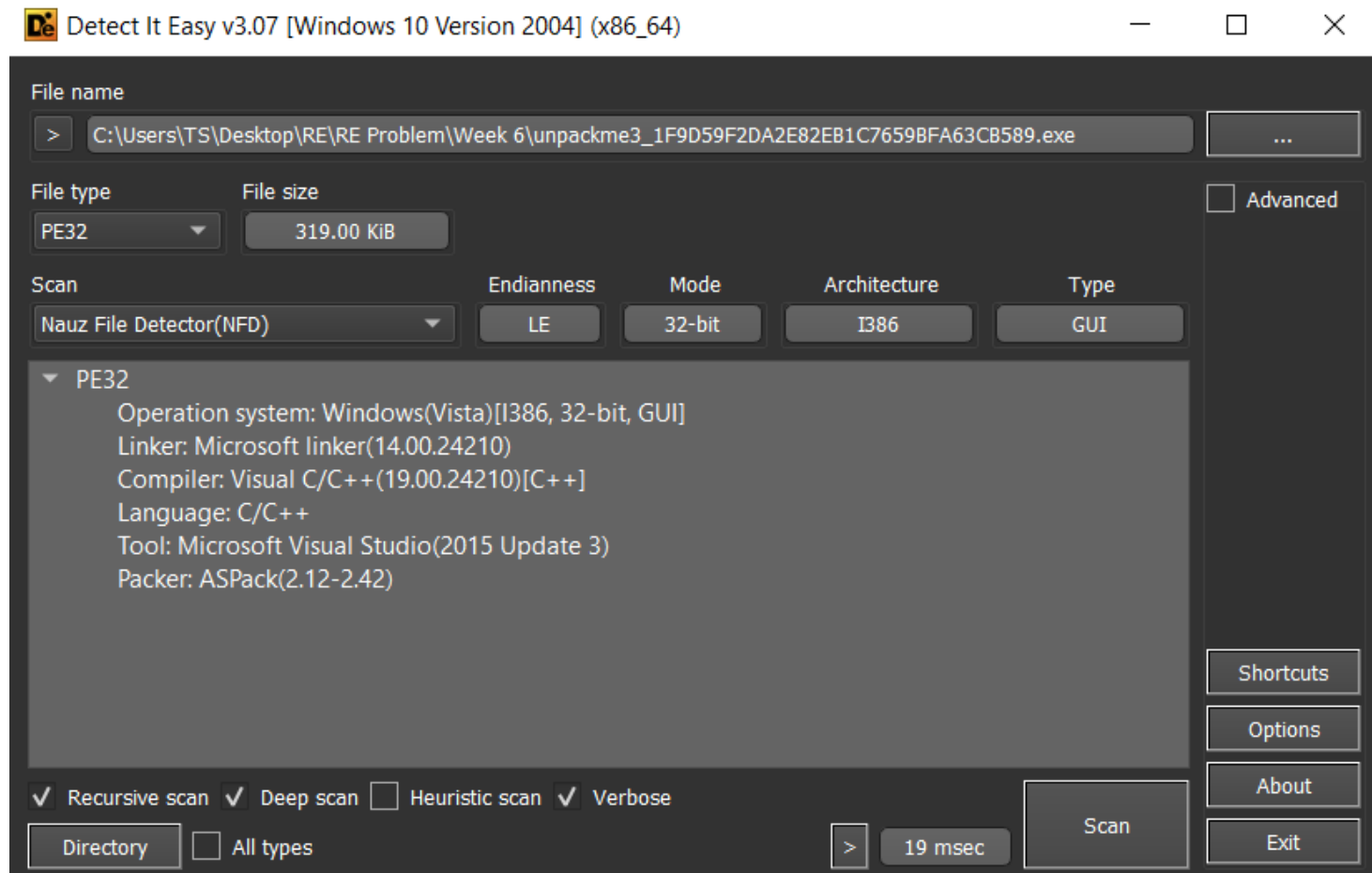
- DialogFunc
- sub\_401050
- WinMain(x,x,x,x)
- pre\_c\_initialization(void)
- sub\_401186
- sub\_40118E
- \_\_srt\_common\_main\_seh(void)
- start
- unknown\_libname\_1
- find\_pe\_section(uchar \* const,uint)
- \_\_srt\_acquire\_startup\_lock
- \_\_srt\_initialize\_crt
- \_\_srt\_initialize\_onexit\_tables
- \_\_srt\_is\_nonwritable\_in\_current\_image
- \_\_srt\_release\_startup\_lock
- \_\_srt\_uninitialize\_crt
- \_onexit
- \_atexit
- \_\_security\_init\_cookie
- sub\_401633
- \_\_get\_startup\_file\_mode
- UserMathErrorFunction
- sub\_401640
- \_\_initialize\_default\_precision
- nullsub\_1

```

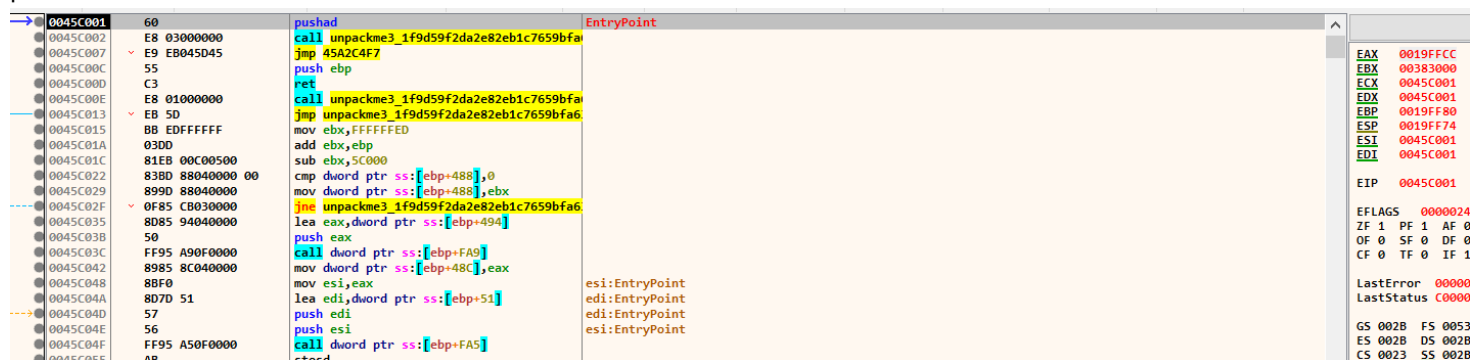
1 int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInsta
2 {
3     INITCOMMONCONTROLSEX picce; // [esp+0h] [ebp-8h] BYREF
4
5     picce.dwSize = 8;
6     picce.dwICC = 255;
7     InitCommonControlsEx(&picce);
8     DialogBoxParamA(hInstance, (LPCSTR)0x65, 0, DialogFunc, 0);
9     return 0;
10 }
  
```

unpackme3\_1F9D59F2DA2E82EB1C7659BFA63CB589.exe

Kiểm tra file bằng Detect It Easy cho thấy file được pack bằng ASPack packer:



Debug file bằng x32dbg và f9 để đến EntryPoint. F7 qua và đặt hardware breakpoint ở địa chỉ ESP đang trỏ sau lệnh pushad.





Dò đến đầu chương trình gốc của file và dump bằng Scylla(xóa import lỗi, dump và fix dump).

The screenshot displays the Scylla x86 v0.9.8 interface. On the left, a list of assembly instructions is shown, including `jmp unpackme3_1f9d59f2da2e82eb1c7659bfa6`, `push ebp`, `mov ebp,esp`, `mov eax,dword ptr ds:[412038]`, `and eax,1F`, `push 20`, `pop ecx`, `sub ecx,eax`, `mov eax,dword ptr ss:[ebp+8]`, `ror eax,c1`, `xor eax,dword ptr ds:[412038]`, `pop ebp`, `ret`, `push ebp`, `mov ebp,esp`, `mov eax,dword ptr ss:[ebp+8]`, `push esi`, `mov ecx,dword ptr ds:[eax+3C]`, `add ecx,eax`, `movzx eax,word ptr ds:[ecx+14]`, `lea edx,dword ptr ds:[ecx+18]`, `add edx,eax`, `movzx eax,word ptr ds:[ecx+6]`, `imul esi,eax,28`, `add esi,edx`, `cmp edx,esi`, `je unpackme3_1f9d59f2da2e82eb1c7659bfa6`, `mov ecx,dword ptr ss:[ebp+C]`, `cmp ecx,dword ptr ds:[edx+C]`, `jb unpackme3_1f9d59f2da2e82eb1c7659bfa6`, `mov eax,dword ptr ds:[edx+8]`, `add eax,dword ptr ds:[edx+C]`, `cmp ecx,eax`, `jb unpackme3_1f9d59f2da2e82eb1c7659bfa6`, and `add edx,28`. The right pane shows the IAT (Import Address Table) with entries for `comctl32.dll (1) FThunk: 0000C000`, `kernel32.dll (64) FThunk: 0000C008`, `user32.dll (5) FThunk: 0000C10C`, and `? (1) FThunk: 0000C124`. The bottom pane shows the log with the message: `IAT Search Adv: Found 71 (0x47) possible IAT entries. IAT Search Adv: Possible IAT first 0040C000 last 0040C124 entry. IAT Search Adv: IAT VA 0040C000 RVA 0000C000 Size 0x0128 (296) IAT Search Nor: IAT VA 0040BFFC RVA 0000BFFC Size 0x0134 (308) IAT parsing finished, found 70 valid APIs, missed 1 APIs. DIRECT IMPORTS - Found 0 possible direct imports with 0 unique APIs!`

Sau đó chạy thành công chương trình gốc.

## unpackme4\_FCEC8D94D5FC3FA6300F5570AB651F3A.exe

Kiểm tra file bằng Detect It Easy cho thấy file được pack bằng FSG packer:

The screenshot displays the Detect It Easy v3.07 [Windows 10 Version 2004] (x86\_64) interface. The file name is `C:\Users\TS\Desktop\RE\RE Problems\Week 6\unpackme4_FCEC8D94D5FC3FA6300F5570AB651F3A.exe`. The file type is `PE32` and the file size is `311.08 KiB`. The base address is `00400000` and the entry point is `00400154`. The interface shows various analysis tools and options, including `File info`, `Memory map`, `Disasm`, `Hex`, `Strings`, `Signatures`, `VirusTotal`, `MIME`, `Search`, `Hash`, `Entropy`, `Extractor`, `PE`, `Export`, `Import`, `Resources`, `.NET`, `TLS`, `Overlay`, `Sections`, `Time date stamp`, `Size of image`, `Resources`, `Manifest`, `Version`, `Scan`, `Endianness`, `Mode`, `Architecture`, `Type`, `Recursive scan`, `Deep scan`, `Heuristic scan`, `Verbose`, `Directory`, `All types`, `Shortcuts`, `Options`, `About`, and `Exit`. The scan results show: `Operation system: Windows(Vista)[I386, 32-bit, GUI]` and `Packer: FSG(2.00)`.

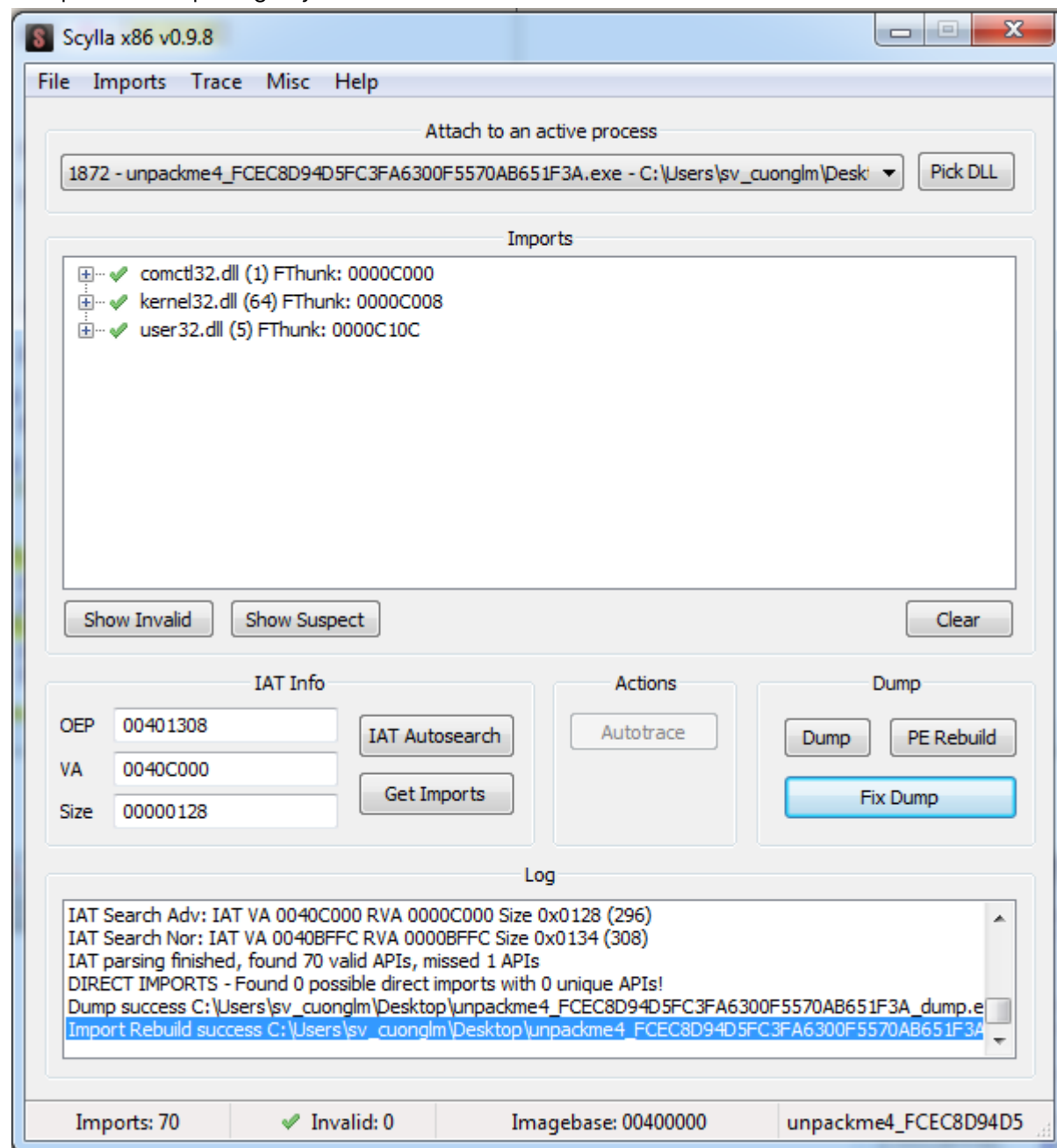
Sau entrypoint có một vòng lặp, đặt breakpoint sau vòng lặp (địa chỉ 0x4001D1) thì nhảy đến OEP:

| CPU | Log | Notes    | Breakpoints | Memory Map | Call Stack | SEH | Script | Symbols | Source                                             | Ref |
|-----|-----|----------|-------------|------------|------------|-----|--------|---------|----------------------------------------------------|-----|
|     |     | 00400198 | 91          |            |            |     |        |         | xchg ecx,eax                                       |     |
|     |     | 00400199 | 48          |            |            |     |        |         | dec eax                                            |     |
|     |     | 0040019A | C1E0 08     |            |            |     |        |         | shl eax,8                                          |     |
|     |     | 0040019D | AC          |            |            |     |        |         | lodsb                                              |     |
|     |     | 0040019E | FF53 04     |            |            |     |        |         | call dword ptr ds:[ebx+4]                          |     |
|     |     | 004001A1 | 3B43 F8     |            |            |     |        |         | cmp eax,dword ptr ds:[ebx-8]                       |     |
|     |     | 004001A4 | 73 0A       |            |            |     |        |         | jae unpackme4_fcce8d94d5fc3fa6300f5570ab651f3a.400 |     |
|     |     | 004001A6 | 80FC 05     |            |            |     |        |         | cmp ah,5                                           |     |
|     |     | 004001A9 | 73 06       |            |            |     |        |         | jae unpackme4_fcce8d94d5fc3fa6300f5570ab651f3a.400 |     |
|     |     | 004001AB | 83F8 7F     |            |            |     |        |         | cmp eax,7F                                         |     |
|     |     | 004001AE | 77 02       |            |            |     |        |         | ja unpackme4_fcce8d94d5fc3fa6300f5570ab651f3a.400  |     |
|     |     | 004001B0 | 41          |            |            |     |        |         | inc ecx                                            |     |
|     |     | 004001B1 | 41          |            |            |     |        |         | inc ecx                                            |     |
|     |     | 004001B2 | 95          |            |            |     |        |         | xchg ebp,eax                                       |     |
|     |     | 004001B3 | 8BC5        |            |            |     |        |         | mov eax,ebp                                        |     |
|     |     | 004001B5 | B6 00       |            |            |     |        |         | mov dh,0                                           |     |
|     |     | 004001B7 | 56          |            |            |     |        |         | push esi                                           |     |
|     |     | 004001B8 | 8BF7        |            |            |     |        |         | mov esi,edi                                        |     |
|     |     | 004001BA | 2BF0        |            |            |     |        |         | sub esi,eax                                        |     |
|     |     | 004001BC | F3:A4       |            |            |     |        |         | rep movsb                                          |     |
|     |     | 004001BE | 5E          |            |            |     |        |         | pop esi                                            |     |
|     |     | 004001BF | EB 9F       |            |            |     |        |         | jmp unpackme4_fcce8d94d5fc3fa6300f5570ab651f3a.400 |     |
|     |     | 004001C1 | 5E          |            |            |     |        |         | pop esi                                            |     |
|     |     | 004001C2 | AD          |            |            |     |        |         | lodsd                                              |     |
|     |     | 004001C3 | 97          |            |            |     |        |         | xchg edi,eax                                       |     |
|     |     | 004001C4 | AD          |            |            |     |        |         | lodsd                                              |     |
|     |     | 004001C5 | 50          |            |            |     |        |         | push eax                                           |     |
|     |     | 004001C6 | FF53 10     |            |            |     |        |         | call dword ptr ds:[ebx+10]                         |     |
|     |     | 004001C9 | 95          |            |            |     |        |         | xchg ebp,eax                                       |     |
|     |     | 004001CA | 8B07        |            |            |     |        |         | mov eax,dword ptr ds:[edi]                         |     |
|     |     | 004001CC | 40          |            |            |     |        |         | inc eax                                            |     |
|     |     | 004001CD | 78 F3       |            |            |     |        |         | js unpackme4_fcce8d94d5fc3fa6300f5570ab651f3a.400  |     |
|     |     | 004001CF | 75 03       |            |            |     |        |         | jne unpackme4_fcce8d94d5fc3fa6300f5570ab651f3a.400 |     |
| EIP |     | 004001D1 | FF63 0C     |            |            |     |        |         | jmp dword ptr ds:[ebx+C]                           |     |

| CPU | Log | Notes    | Breakpoints   | Memory Map | Call Stack | SEH | Script | Symbols | Source                                              | References | Threads | Handles | Trace |
|-----|-----|----------|---------------|------------|------------|-----|--------|---------|-----------------------------------------------------|------------|---------|---------|-------|
|     |     | 00401308 | E8 8A020000   |            |            |     |        |         | call unpackme4_fcce8d94d5fc3fa6300f5570ab651f3a.400 |            |         |         |       |
|     |     | 00401312 | E9 8EFFFFFF   |            |            |     |        |         | jmp unpackme4_fcce8d94d5fc3fa6300f5570ab651f3a.400  |            |         |         |       |
|     |     | 00401313 | 55            |            |            |     |        |         | push ebp                                            |            |         |         |       |
|     |     | 00401315 | 88EC          |            |            |     |        |         | mov ebp,esp                                         |            |         |         |       |
|     |     | 00401315 | A1 38204100   |            |            |     |        |         | mov eax,dword ptr ds:[412038]                       |            |         |         |       |
|     |     | 0040131A | 83E0 1F       |            |            |     |        |         | and eax,1F                                          |            |         |         |       |
|     |     | 0040131D | 6A 20         |            |            |     |        |         | push 20                                             |            |         |         |       |
|     |     | 0040131F | 59            |            |            |     |        |         | pop ecx                                             |            |         |         |       |
|     |     | 00401320 | 28C8          |            |            |     |        |         | sub ecx,eax                                         |            |         |         |       |
|     |     | 00401322 | 8B45 08       |            |            |     |        |         | mov eax,dword ptr ss:[ebp+8]                        |            |         |         |       |
|     |     | 00401325 | D3C8          |            |            |     |        |         | ror eax,cl                                          |            |         |         |       |
|     |     | 00401327 | 3305 38204100 |            |            |     |        |         | xor eax,dword ptr ds:[412038]                       |            |         |         |       |
|     |     | 0040132D | 5D            |            |            |     |        |         | pop ebp                                             |            |         |         |       |
|     |     | 0040132E | C3            |            |            |     |        |         | ret                                                 |            |         |         |       |
|     |     | 0040132F | 55            |            |            |     |        |         | push ebp                                            |            |         |         |       |
|     |     | 00401330 | 88EC          |            |            |     |        |         | mov ebp,esp                                         |            |         |         |       |
|     |     | 00401332 | 8B45 08       |            |            |     |        |         | mov eax,dword ptr ss:[ebp+8]                        |            |         |         |       |
|     |     | 00401335 | 56            |            |            |     |        |         | push esi                                            |            |         |         |       |
|     |     | 00401336 | 8B48 3C       |            |            |     |        |         | mov ecx,dword ptr ds:[eax+3C]                       |            |         |         |       |
|     |     | 00401339 | 03C8          |            |            |     |        |         | add ecx,eax                                         |            |         |         |       |
|     |     | 0040133B | 0FB741 14     |            |            |     |        |         | movzx eax,word ptr ds:[ecx+14]                      |            |         |         |       |
|     |     | 0040133F | 8D51 18       |            |            |     |        |         | lea edx,dword ptr ds:[ecx+18]                       |            |         |         |       |
|     |     | 00401342 | 03D0          |            |            |     |        |         | add edx,eax                                         |            |         |         |       |
|     |     | 00401344 | 0FB741 06     |            |            |     |        |         | movzx eax,word ptr ds:[ecx+6]                       |            |         |         |       |
|     |     | 00401348 | 6BF0 28       |            |            |     |        |         | imul esi,eax,28                                     |            |         |         |       |
|     |     | 0040134B | 03F2          |            |            |     |        |         | add esi,edx                                         |            |         |         |       |
|     |     | 0040134D | 3BD6          |            |            |     |        |         | cmp edx,esi                                         |            |         |         |       |
|     |     | 0040134F | 74 19         |            |            |     |        |         | je unpackme4_fcce8d94d5fc3fa6300f5570ab651f3a.401   |            |         |         |       |
|     |     | 00401351 | 8B4D 0C       |            |            |     |        |         | mov ecx,dword ptr ss:[ebp+C]                        |            |         |         |       |
|     |     | 00401354 | 3B4A 0C       |            |            |     |        |         | cmp ecx,dword ptr ds:[edx+C]                        |            |         |         |       |
|     |     | 00401357 | 72 0A         |            |            |     |        |         | jnb unpackme4_fcce8d94d5fc3fa6300f5570ab651f3a.401  |            |         |         |       |
|     |     | 00401359 | 8B42 08       |            |            |     |        |         | mov eax,dword ptr ds:[edx+8]                        |            |         |         |       |
|     |     | 0040135C | 0342 0C       |            |            |     |        |         | add eax,dword ptr ds:[edx+C]                        |            |         |         |       |
|     |     | 0040135F | 3BC8          |            |            |     |        |         | cmp ecx,eax                                         |            |         |         |       |
|     |     | 00401361 | 72 0C         |            |            |     |        |         | jb unpackme4_fcce8d94d5fc3fa6300f5570ab651f3a.401   |            |         |         |       |



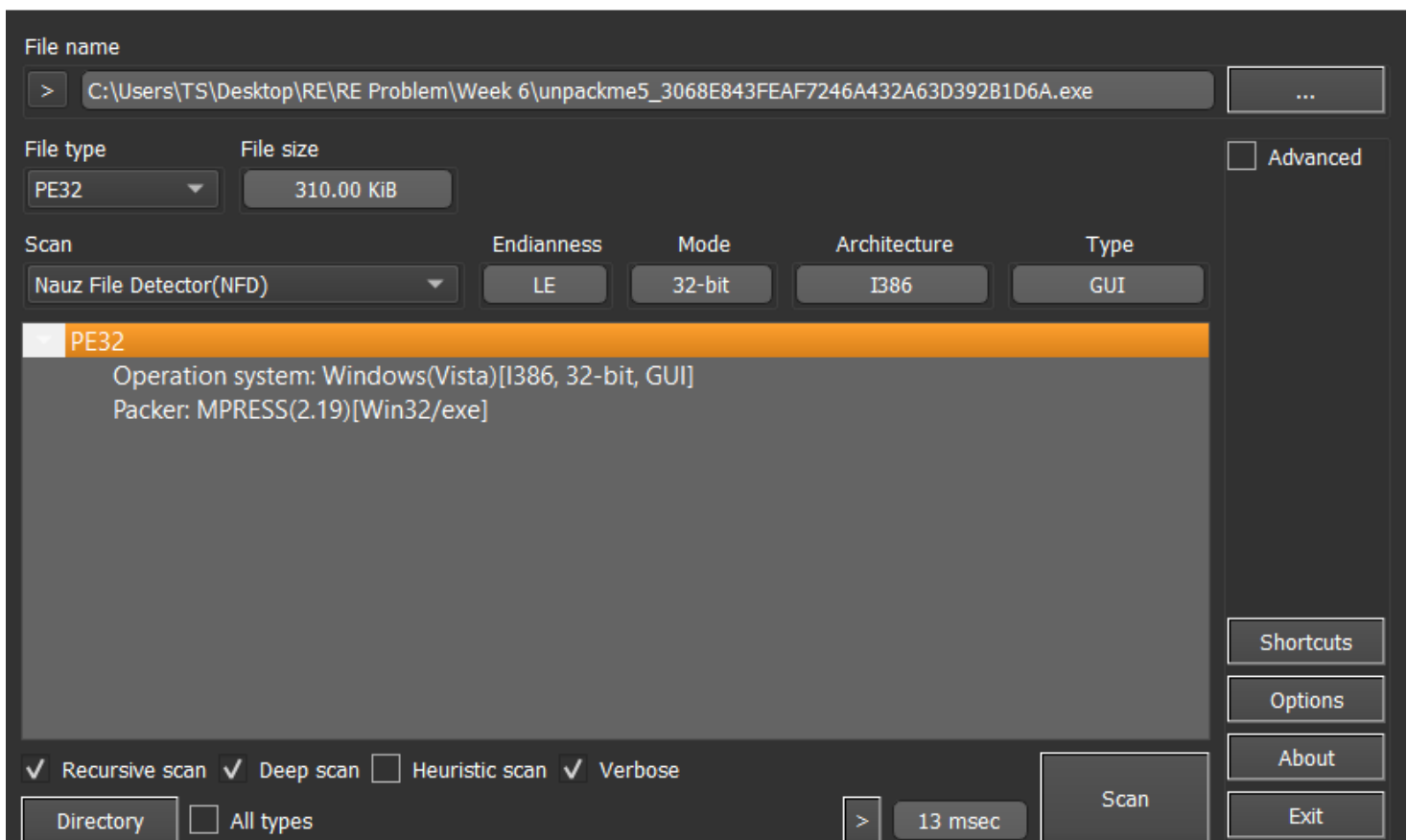
Dump và fix dump bằng Scylla:



**unpackme5\_3068E843FEAF7246A432A63D392B1D6A.exe**

Làm tương tự unpack3.

Kiểm tra file bằng Detect It Easy cho thấy file được pack bằng MPRESS packer:



Debug file bằng x32dbg và f9 để đến EntryPoint. F7 qua và đặt hardware breakpoint ở địa chỉ ESP đang trỏ(sau lệnh pushad):

|   |          |             |                                          |                                |
|---|----------|-------------|------------------------------------------|--------------------------------|
| → | 0045C0E4 | 60          | pushad                                   | EntryPoint                     |
|   | 0045C0E5 | E8 00000000 | call unpackme5_3068e843feaf7246a432a63d3 | call \$0                       |
|   | 0045C0EA | 58          | pop eax                                  |                                |
|   | 0045C0EB | 05 5A0B0000 | add eax,B5A                              |                                |
|   | 0045C0F0 | 8B30        | mov esi,dword ptr ds:[eax]               | esi:EntryPoint                 |
|   | 0045C0F2 | 03F0        | add esi,eax                              | esi:EntryPoint                 |
|   | 0045C0F4 | 2BC0        | sub eax,eax                              |                                |
|   | 0045C0F6 | 8BFE        | mov edi,esi                              | edi:EntryPoint, esi:EntryPoint |
|   | 0045C0F8 | 66:AD       | lodsw                                    |                                |
|   | 0045C0FA | C1E0 0C     | shl eax,C                                |                                |
|   | 0045C0FD | 8BC8        | mov ecx,eax                              | ecx:EntryPoint                 |
|   | 0045C0FF | 50          | push eax                                 |                                |
|   | 0045C100 | AD          | lodsd                                    |                                |
|   | 0045C101 | 2BC8        | sub ecx,eax                              | ecx:EntryPoint                 |
|   | 0045C103 | 03F1        | add esi,ecx                              | esi:EntryPoint, ecx:EntryPoint |
|   | 0045C105 | 8BC8        | mov ecx,eax                              | ecx:EntryPoint                 |
|   | 0045C107 | 57          | push edi                                 | edi:EntryPoint                 |
|   | 0045C108 | 51          | push ecx                                 | ecx:EntryPoint                 |
|   | 0045C109 | 49          | dec ecx                                  | ecx:EntryPoint                 |
|   | 0045C10A | 8A4439 06   | mov al,byte ptr ds:[ecx+edi+6]           |                                |
|   | 0045C10E | 880431      | mov byte ptr ds:[ecx+esi],al             |                                |
|   | 0045C111 | 75 F6       | jne unpackme5_3068e843feaf7246a432a63d39 |                                |
|   | 0045C113 | 2BC0        | sub eax,eax                              |                                |
|   | 0045C115 | AC          | lodsb                                    |                                |

Dò đến đầu chương trình gốc của file và dump bằng Scylla (xóa import lỗi, dump và fix dump).

The screenshot displays the Scylla x86 v0.9.8 application. The left pane shows assembly code for a file named 'ie843feaf7246a432a63d392b1d6a.exe'. The code includes instructions like 'call unpackme5\_3068e843feaf7246a432a63d392b1d6a.exe', 'push ebp', 'mov ebp,esp', 'mov eax,dword ptr ds:[412038]', 'and eax,1F', 'push 20', 'pop ecx', 'sub ecx,eax', 'mov eax,dword ptr ss:[ebp+8]', 'ror eax,cl', 'xor eax,dword ptr ds:[412038]', 'pop ebp', 'ret', 'push ebp', 'mov ebp,esp', 'mov eax,dword ptr ss:[ebp+8]', 'push esi', 'mov ecx,dword ptr ds:[eax+3C]', 'add ecx,eax', 'movzx eax,word ptr ds:[ecx+14]', 'lea edx,dword ptr ds:[ecx+18]', 'add edx,eax', 'movzx eax,word ptr ds:[ecx+6]', 'imul esi,eax,28', 'add esi,edx', 'cmp edx,esi', 'je unpackme5\_3068e843feaf7246a432a63d392b1d6a.exe', 'mov ecx,dword ptr ss:[ebp+C]', 'cmp ecx,dword ptr ds:[edx+C]', 'jb unpackme5\_3068e843feaf7246a432a63d392b1d6a.exe', 'mov eax,dword ptr ds:[edx+8]', 'add eax,dword ptr ds:[edx+C]', 'cmp ecx,eax', 'jb unpackme5\_3068e843feaf7246a432a63d392b1d6a.exe'. The right pane shows the 'Imports' section with a list of imported DLLs: 'comctl32.dll (1) FThunk: 0000C000', 'kernel32.dll (64) FThunk: 0000C008', and 'user32.dll (5) FThunk: 0000C10C'. Below the imports, there are buttons for 'Show Invalid', 'Show Suspect', 'Clear', 'Autotrace', 'Dump', 'PE Rebuild', and 'Fix Dump'. The 'Log' section at the bottom shows the results of the import search and the success of the import rebuild.

## unpackme6\_FD07CFEAB4F73C6759FFB4554B0068C8.exe

Phân tích bằng PEiD cho thấy file pack bằng VMProtect packer:

The screenshot shows the Detect It Easy v3.07 [Windows 10 Version 2004] (x86\_64) interface. The 'File name' field contains 'C:\Users\TS\Desktop\RE\RE Problems\Week 6\unpackme6\_FD07CFEAB4F73C6759FFB4554B0068C8.exe'. The 'File type' is 'PE32' and the 'File size' is '2.39 MIB'. The 'Scan' section shows 'Nauz File Detector(NFD)' as the scanner, with 'Endianness' set to 'LE', 'Mode' set to '32-bit', 'Architecture' set to 'I386', and 'Type' set to 'GUI'. The 'PE32' section provides detailed information: 'Operation system: Windows(XP)[I386, 32-bit, GUI]', 'Linker: Microsoft linker(14.00.24210)', 'Compiler: Visual C/C++(19.00.24210)[C++]', 'Language: C/C++', 'Tool: Microsoft Visual Studio(2015 Update 3)', and 'Protector: VMProtect(3.0.9)'. At the bottom, there are checkboxes for 'Recursive scan', 'Deep scan', 'Heuristic scan', and 'Verbose', along with a 'Directory' checkbox and 'All types' checkbox. The 'Scan' button is highlighted, and the '23 msec' time is displayed.

Debug file x64dbg và đặt breakpoint ở kernel32.VirtualProtect:

| CPU      | Log                            | Notes  | Breakpoints                        | Memory Map | Call Stack | SEH     | Script                      | Symbols | Source | References |
|----------|--------------------------------|--------|------------------------------------|------------|------------|---------|-----------------------------|---------|--------|------------|
| Base     | Module                         | Party  | Path                               | Address    | Type       | Ordinal | Symbol                      |         |        |            |
| 00150000 | unpackme6_fd07cfeab4f73c6759ff | User   | C:\Users\TS\Desktop\RE\R           | 75D004C0   | Export     | 1490    | VirtualProtect              |         |        |            |
| 74070000 | wtapi32.dll                    | System | C:\Windows\SysWow64\wtapi32.dll    | 75D15D50   | Export     | 1491    | VirtualProtectEx            |         |        |            |
| 751A0000 | comctl32.dll                   | System | C:\Windows\WinSxS\x86_mi           | 75D61364   | Import     |         | kernelbase.VirtualProtect   |         |        |            |
| 753B0000 | ucrtbase.dll                   | System | C:\Windows\SysWow64\ucrtbase.dll   | 75D6138C   | Import     |         | kernelbase.VirtualProtectEx |         |        |            |
| 755C0000 | imm32.dll                      | System | C:\Windows\SysWow64\imm32.dll      |            |            |         |                             |         |        |            |
| 757A0000 | advapi32.dll                   | System | C:\Windows\SysWow64\advapi32.dll   |            |            |         |                             |         |        |            |
| 75820000 | win32u.dll                     | System | C:\Windows\SysWow64\win32u.dll     |            |            |         |                             |         |        |            |
| 75CE0000 | kernel32.dll                   | System | C:\Windows\SysWow64\kernel32.dll   |            |            |         |                             |         |        |            |
| 76390000 | msvcrt.dll                     | System | C:\Windows\SysWow64\msvcrt.dll     |            |            |         |                             |         |        |            |
| 76470000 | rpcrt4.dll                     | System | C:\Windows\SysWow64\rpcrt4.dll     |            |            |         |                             |         |        |            |
| 76530000 | sechost.dll                    | System | C:\Windows\SysWow64\sechost.dll    |            |            |         |                             |         |        |            |
| 765B0000 | msvcrt.dll                     | System | C:\Windows\SysWow64\msvcrt.dll     |            |            |         |                             |         |        |            |
| 76670000 | gdi32.dll                      | System | C:\Windows\SysWow64\gdi32.dll      |            |            |         |                             |         |        |            |
| 76870000 | kernelbase.dll                 | System | C:\Windows\SysWow64\kernelbase.dll |            |            |         |                             |         |        |            |
| 76B40000 | user32.dll                     | System | C:\Windows\SysWow64\user32.dll     |            |            |         |                             |         |        |            |
| 774B0000 | gdi32.dll                      | System | C:\Windows\SysWow64\gdi32.dll      |            |            |         |                             |         |        |            |
| 774F0000 | ntdll.dll                      | System | C:\Windows\SysWow64\ntdll.dll      |            |            |         |                             |         |        |            |

Search: Type here to filter results... ☐ Regex Search: VirtualProtect

No symbols loaded for: msvcrtdll

IDIA! Skipping non-existent PDB: C:\Users\TS\Desktop\Archive\release\x32\symbols\wtapi32.pdb\620F26C29E03BE7B833AF38919856B731\wtapi32.pdb

,sau đó F9 8 lần. Sau đó code sẽ được giải nén ở .text. đặt memory breakpoint ở .text và F9 đến khi tìm được OEP đúng là 0xF11308, dump ra bằng Scylla:

00F11308

E8 8A020000

call unpackme6\_fd07cfeab4f73c6759ffb4554b0

00F1130D

E9 BEFEFFFF

jmp unpackme6\_fd07cfeab4f73c6759ffb4554b0

00F11312

55

push ebp

00F11313

8B45 08

mov ebp,esp

00F1131A

83E0 1F

and eax,1F

00F1131D

6A 20

push 20

00F1131F

59

pop ecx

00F11320

2BC8

sub ecx,eax

00F11322

8B45 08

mov eax,dword ptr ds:[ebp+8]

00F11325

D3C8

ror eax,cl

00F11327

3305 3820F200

xor eax,dword ptr ds:[F22038]

00F1132D

5D

pop ebp

00F1132E

C3

ret

00F1132F

55

push ebp

00F11330

8BEC

mov ebp,esp

00F11332

8B45 08

mov eax,dword ptr ss:[ebp+8]

00F11335

56

push esi

00F11336

8B48 3C

mov ecx,dword ptr ds:[eax+3C]

00F11339

03C8

add ecx,eax

00F1133B

0FB741 14

movzx eax,word ptr ds:[ecx+14]

00F1133F

8D51 18

lea edx,dword ptr ds:[ecx+18]

00F11342

03D0

add edx,eax

00F11344

0FB741 06

movzx eax,word ptr ds:[ecx+6]

00F11348

68F0 28

imul esi,eax,28

00F1134B

03F2

add esi,edx

00F1134D

3B06

cmp edx,esi

00F1134F

74 19

jbe unpackme6\_fd07cfeab4f73c6759ffb4554b0

00F11351

8B4D 0C

mov ecx,dword ptr ss:[ebp+C]

00F11354

3B4A 0C

cmp ecx,dword ptr ds:[edx+C]

00F11357

72 0A

jbe unpackme6\_fd07cfeab4f73c6759ffb4554b0

00F11359

8B4D 08

mov eax,dword ptr ds:[edx+8]

00F1135C

0342 0C

add eax,dword ptr ds:[edx+C]

00F1135F

3BC8

cmp ecx,eax

00F11361

72 0C

jbe unpackme6\_fd07cfeab4f73c6759ffb4554b0

File

Imports

Trace

Misc

Help

Attach to an active process

1132 - unpackme6\_F0D7CFEAB4F73C6759FFB4554B0068C8.exe - C:\Users\TS\Desktop\RE\R

Pick DLL

Imports

(1) FThunk: 0000C124

Show Invalid

Show Suspect

Clear

IAT Info

Actions

Dump

OEP 00F11308

IAT Autosearch

Autotrace

Dump

PE Rebuild

VA 00F1C124

Get Imports

Fix Dump

Size 00000004

Log

IAT Search Adv: Found 1 (0x1) possible IAT entries.

IAT Search Adv: Possible IAT first 00F1C124 last 00F1C124 entry.

IAT Search Adv: IAT VA 00F1C124 RVA 0000C124 Size 0x0004 (4)

IAT Search Nor: IAT not found at OEP 00F11308!

IAT parsing finished, found 0 valid APIs, missed 1 APIs

DIRECT IMPORTS - Found 0 possible direct imports with 0 unique APIs!

iffb4554b0068c8.00F111A0

07cfeab4f73c6759ffb4554b0068c8.exe:\$130D #0

Dump 3

Dump 4

Dump 5

Watch 1

Locals

Stru

54 77 14 00 16 00 78 74 64 77

54 77 0E 00 10 00 00 7E 64 77

ASCII

....(|dw...xt dw

....ü|dw....~dw

Phân tích tĩnh được code đã dump nhưng file không chạy được vì IAT bị hỏng:

The screenshot displays the IDA Pro interface with two main panes. The left pane, titled 'Functions', shows a list of functions. The right pane, titled 'Pseudocode-A', shows the pseudocode for the selected function, 'start'.

**Functions List:**

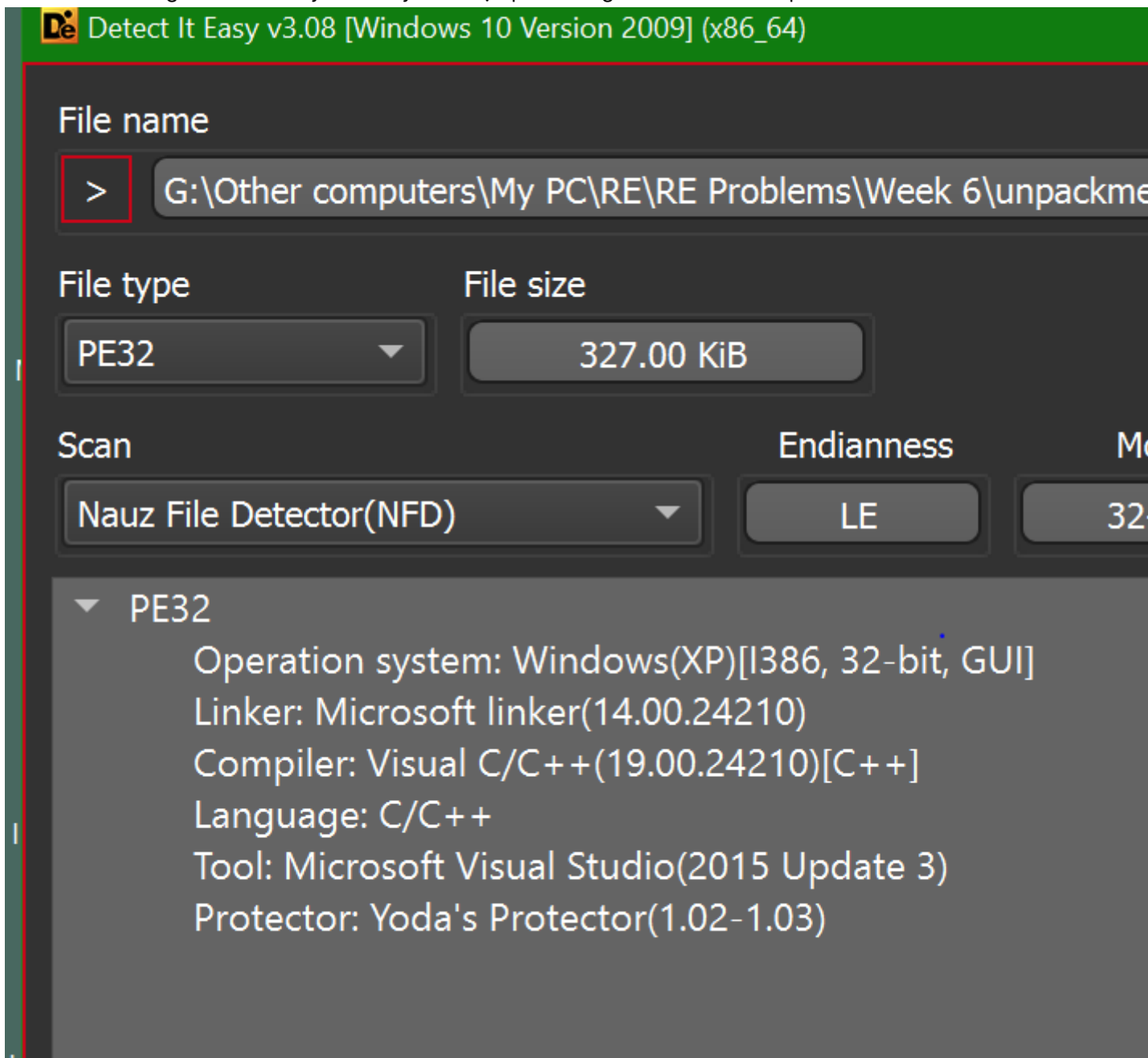
- sub\_F11000
- sub\_F11050
- nullsub\_67
- nullsub\_45
- WinMain(x,x,x,x)
- pre\_c\_initialization(void)
- \_\_srt\_common\_main\_seh(void)
- start**
- unknown\_libname\_1
- find\_pe\_section(uchar \* const,uint)
- \_\_srt\_acquire\_startup\_lock
- \_\_srt\_initialize\_crt
- \_\_srt\_initialize\_onexit\_tables
- \_\_srt\_is\_nonwritable\_in\_current\_image
- \_\_srt\_release\_startup\_lock
- \_\_srt\_uninitialize\_crt
- \_onexit
- \_atexit
- \_\_security\_init\_cookie
- sub\_F11633
- \_\_get\_startup\_file\_mode
- UserMathErrorFunction
- sub\_F11640
- \_\_initialize\_default\_precision
- \_guard\_check\_icall\_nop(x)
- sub\_F1166E
- sub\_F11674
- \_\_srt\_initialize\_default\_local\_stdio\_opt
- sub\_F11697
- sub\_F116A3

**Pseudocode for 'start':**

```
1 int start()
2 {
3     __security_init_cookie();
4     return __srt_common_main_seh();
5 }
```

unpackme7\_1998BC713BE5132B9356438D53CAE971.exe

Kiểm tra file bằng Detect It Easy cho thấy file được pack bằng Yoda's Protector packer:



Tính năng của Yoda's Protector:

- Anti debugging: JMP vào giữa một hàm, raise exception INT 3, BlockInput(), IsDebuggerPresent(), BlockInput(), CreateToolhelp32Snapshot(), Process32First(), và Process32Next(), GetCurrentProcessId(),...
- Anti-SoftICE
- Chống sửa đổi(Checksum Check)
- Load API bằng LoadLibraryA() và GetProcAddress()
- Chống dump
- Xóa thông tin Import
- Xóa PE header

(ref: <https://sanseolab.tistory.com/11>)

File chỉ chạy trên Windows XP. Dùng x32dbg để chạy chương trình sẽ bị thoát ra do chương trình phát hiện debugger. Khắc phục bằng cách đặt breakpoint ở hàm LoadLibraryA(), chạy đến khi chương trình load đầy đủ thư viện:



| CPU                                    | Log                                        | Notes  | Breakpoints                             | Memory Map | Call Stack | SEH     | Script     | Symbols                        | Source         | References | Threads |
|----------------------------------------|--------------------------------------------|--------|-----------------------------------------|------------|------------|---------|------------|--------------------------------|----------------|------------|---------|
| Base                                   | Module                                     | Party  | Path                                    | Address    | Type       | Ordinal | Symbol     |                                |                |            |         |
| 00400000                               | unpackme7_1998bc713be5132b9356438d53cae971 | User   | C:\Documents and Settings\RagdollFan20  | 7E46CA7E   | Export     | 15      | BlockInput |                                |                |            |         |
| 68000000                               | rsaenh.dll                                 | System | C:\WINDOWS\system32\rsaenh.dll          |            |            |         |            |                                |                |            |         |
| 76390000                               | imm32.dll                                  | System | C:\WINDOWS\system32\imm32.dll           |            |            |         |            |                                |                |            |         |
| 773D0000                               | comctl32.dll                               | System | C:\WINDOWS\WinSxS\x86_Microsoft.Windows |            |            |         |            |                                |                |            |         |
| 77C10000                               | msvcrt.dll                                 | System | C:\WINDOWS\system32\msvcrt.dll          |            |            |         |            |                                |                |            |         |
| 77DD0000                               | advapi32.dll                               | System | C:\WINDOWS\system32\advapi32.dll        |            |            |         |            |                                |                |            |         |
| 77E70000                               | rpcrt4.dll                                 | System | C:\WINDOWS\system32\rpcrt4.dll          |            |            |         |            |                                |                |            |         |
| 77F10000                               | gdi32.dll                                  | System | C:\WINDOWS\system32\gdi32.dll           |            |            |         |            |                                |                |            |         |
| 77F60000                               | shlwapi.dll                                | System | C:\WINDOWS\system32\shlwapi.dll         |            |            |         |            |                                |                |            |         |
| 77FE0000                               | secur32.dll                                | System | C:\WINDOWS\system32\secur32.dll         |            |            |         |            |                                |                |            |         |
| 7C800000                               | kernel32.dll                               | System | C:\WINDOWS\system32\kernel32.dll        |            |            |         |            |                                |                |            |         |
| 7C900000                               | ntdll.dll                                  | System | C:\WINDOWS\system32\ntdll.dll           |            |            |         |            |                                |                |            |         |
| 7E410000                               | user32.dll                                 | System | C:\WINDOWS\system32\user32.dll          |            |            |         |            |                                |                |            |         |
| Search: Type here to filter results... |                                            |        |                                         |            |            |         |            | <input type="checkbox"/> Regex | Search: BlockI |            |         |

Patch nop hàm BlockInput(), patch xor eax, eax IsDebuggerPresent(), patch mov eax, {pid của x64 dbg} trong GetCurrentProcessId() để bypass:

|          |         |       |            |
|----------|---------|-------|------------|
| 7E46CA7E | 90      | nop   | BlockInput |
| 7E46CA7F | 90      | nop   |            |
| 7E46CA80 | 90      | nop   |            |
| 7E46CA81 | 90      | nop   |            |
| 7E46CA82 | 90      | nop   |            |
| 7E46CA83 | 90      | nop   |            |
| 7E46CA84 | 90      | nop   |            |
| 7E46CA85 | 90      | nop   |            |
| 7E46CA86 | 90      | nop   |            |
| 7E46CA87 | 90      | nop   |            |
| 7E46CA88 | 90      | nop   |            |
| 7E46CA89 | 90      | nop   |            |
| 7E46CA8A | C2 0400 | ret 4 |            |

|          |             |              |                     |
|----------|-------------|--------------|---------------------|
| 7C8099C0 | 90          | nop          | GetCurrentProcessId |
| 7C8099C1 | 90          | nop          |                     |
| 7C8099C2 | 90          | nop          |                     |
| 7C8099C3 | B8 8D030000 | mov eax, 38D |                     |
| 7C8099C8 | 90          | nop          |                     |
| 7C8099C9 | C3          | ret          |                     |

|          |      |              |                   |
|----------|------|--------------|-------------------|
| 7C82F6EF | 90   | nop          | IsDebuggerPresent |
| 7C82F6F0 | 90   | nop          |                   |
| 7C82F6F1 | 90   | nop          |                   |
| 7C82F6F2 | 90   | nop          |                   |
| 7C82F6F3 | 90   | nop          |                   |
| 7C82F6F4 | 90   | nop          |                   |
| 7C82F6F5 | 90   | nop          |                   |
| 7C82F6F6 | 90   | nop          |                   |
| 7C82F6F7 | 90   | nop          |                   |
| 7C82F6F8 | 33C0 | xor eax, eax |                   |
| 7C82F6FA | 90   | nop          |                   |
| 7C82F6FB | 90   | nop          |                   |
| 7C82F6FC | C3   | ret          |                   |

Hoặc đơn giản hơn là dùng plugin ScyllaHide để debugger không bị phát hiện. Khi debug với ScyllaHide, f9 9 lần thì chương trình chạy ra cửa sổ, do vậy OEP được chạy giữa lần f9 thứ 8 và 9. f9 8 lần đến đây rồi đặt memory access breakpoint tại section không tên đầu tiên(khả năng cao là .text):

|          |          |      |                     |
|----------|----------|------|---------------------|
| 00401000 | 0000B000 | User | " "                 |
| 0040C000 | 00006000 | User | " "                 |
| 00412000 | 00002000 | User | " "                 |
| 00414000 | 00001000 | User | " "                 |
| 00415000 | 00046000 | User | ".rsrc"             |
| 0045B000 | 00009000 | User | ".vcs"              |
| 00470000 | 00001000 | User |                     |
| 00480000 | 00001000 | User |                     |
| 00490000 | 00001000 | User |                     |
| 004A0000 | 00001000 | User |                     |
| 004B0000 | 00001000 | User |                     |
| 004C0000 | 00001000 | User |                     |
| 004D0000 | 00001000 | User |                     |
| 004E0000 | 00001000 | User |                     |
| 004F0000 | 00001000 | User |                     |
| 00500000 | 00002000 | User |                     |
| 00502000 | 000BE000 | User | Reserved (00500000) |
| 005C0000 | 00002000 | User |                     |
| 005C2000 | 00006000 | User | Reserved (00500000) |
| 005D0000 | 00103000 | User |                     |
| 006E0000 | 00001000 | User |                     |
| 006F0000 | 0003B000 | User |                     |
| 0072B000 | 002C5000 | User | Reserved (006F0000) |
| 009F0000 | 00001000 | User |                     |
| 00A00000 | 00004000 | User |                     |

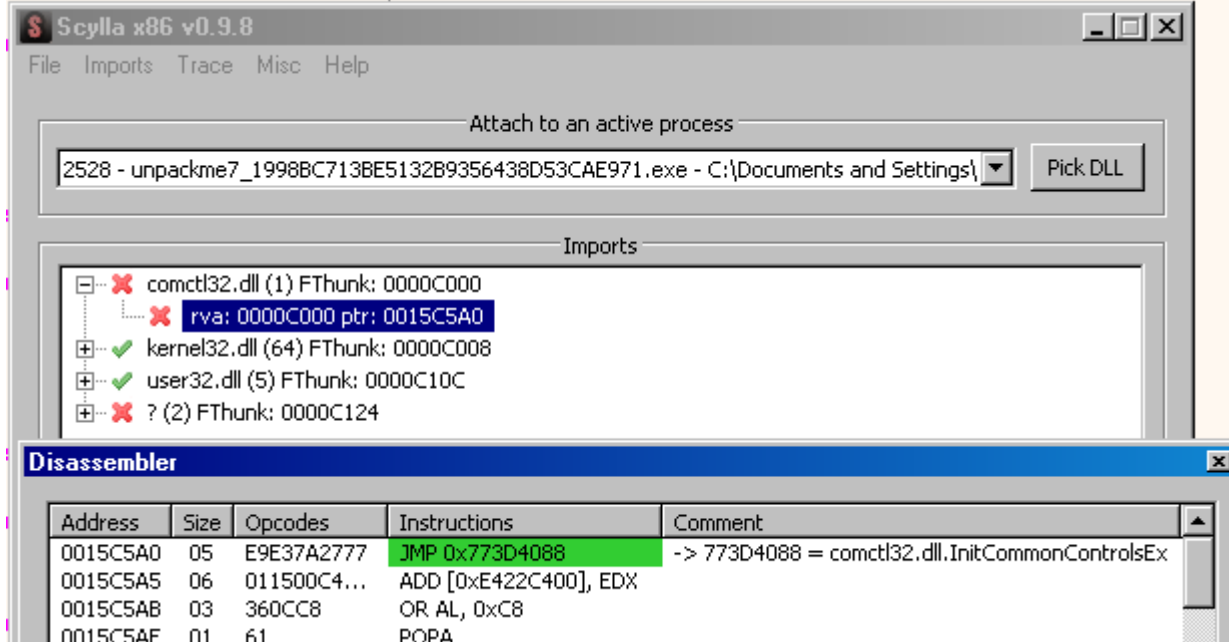
Follow in Disassembler  
Follow in Dump  
Follow in Symbols  
Dump Memory to File  
Comment  
Find Pattern... Ctrl+B  
Switch View  
Find references to region  
Allocate memory  
Free memory  
Go to  
Set Page Memory Rights  
**Memory Breakpoint**  
Copy

Access  
Read  
Write  
Execute

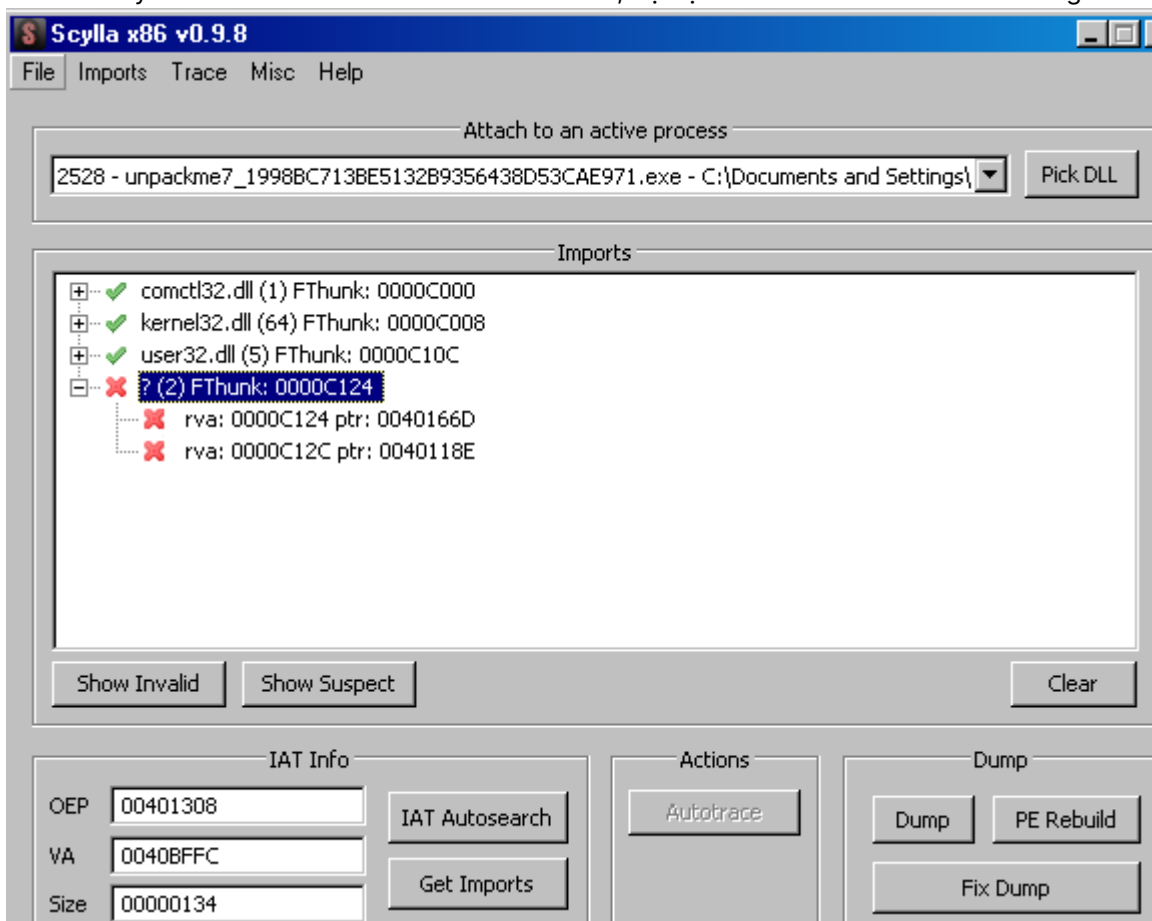
Chương trình dừng tại địa chỉ 0x401308, chính là OEP:

|            |               |                                          |
|------------|---------------|------------------------------------------|
| → 00401308 | E8 8A020000   | call unpackme7_1998bc713be5132b9356438d5 |
| 0040130D   | ^ E9 8EFEFFFF | jmp unpackme7_1998bc713be5132b9356438d5  |
| 00401312   | 55            | push ebp                                 |
| 00401313   | 8BEC          | mov ebp,esp                              |
| 00401315   | A1 38204100   | mov eax,dword ptr ds:[412038]            |
| 0040131A   | 83E0 1F       | and eax,1F                               |
| 0040131D   | 6A 20         | push 20                                  |
| 0040131F   | 59            | pop ecx                                  |
| 00401320   | 2BC8          | sub ecx,eax                              |
| 00401322   | 8B45 08       | mov eax,dword ptr ss:[ebp+8]             |
| 00401325   | D3C8          | ror eax,cl                               |
| 00401327   | 3305 38204100 | xor eax,dword ptr ds:[412038]            |
| 0040132D   | 5D            | pop ebp                                  |
| 0040132E   | C3            | ret                                      |
| 0040132F   | 55            | push ebp                                 |
| 00401330   | 8BEC          | mov ebp,esp                              |
| 00401332   | 8B45 08       | mov eax,dword ptr ss:[ebp+8]             |
| 00401335   | 56            | push esi                                 |
| 00401336   | 8B48 3C       | mov ecx,dword ptr ds:[eax+3C]            |
| 00401339   | 03C8          | add ecx,eax                              |
| 0040133B   | 0FB741 14     | movzx eax,word ptr ds:[ecx+14]           |
| 0040133F   | 8D51 18       | lea edx,dword ptr ds:[ecx+18]            |
| 00401342   | 03D0          | add edx,eax                              |
| 00401344   | 0FB741 06     | movzx eax,word ptr ds:[ecx+6]            |

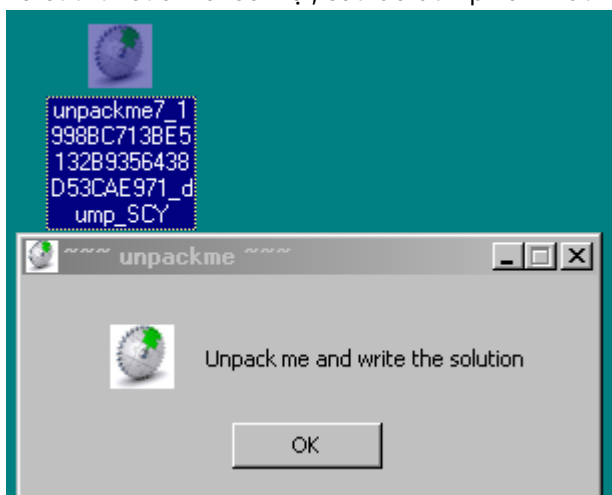
Dùng Scylla IAT Auto Search chế độ normal(chế độ advanced gặp lỗi), get imports và disassemble function chưa được nhận diện:



→ Cho thấy function trên là InitCommonControlEx, đặt lại con trỏ của function cho đúng:

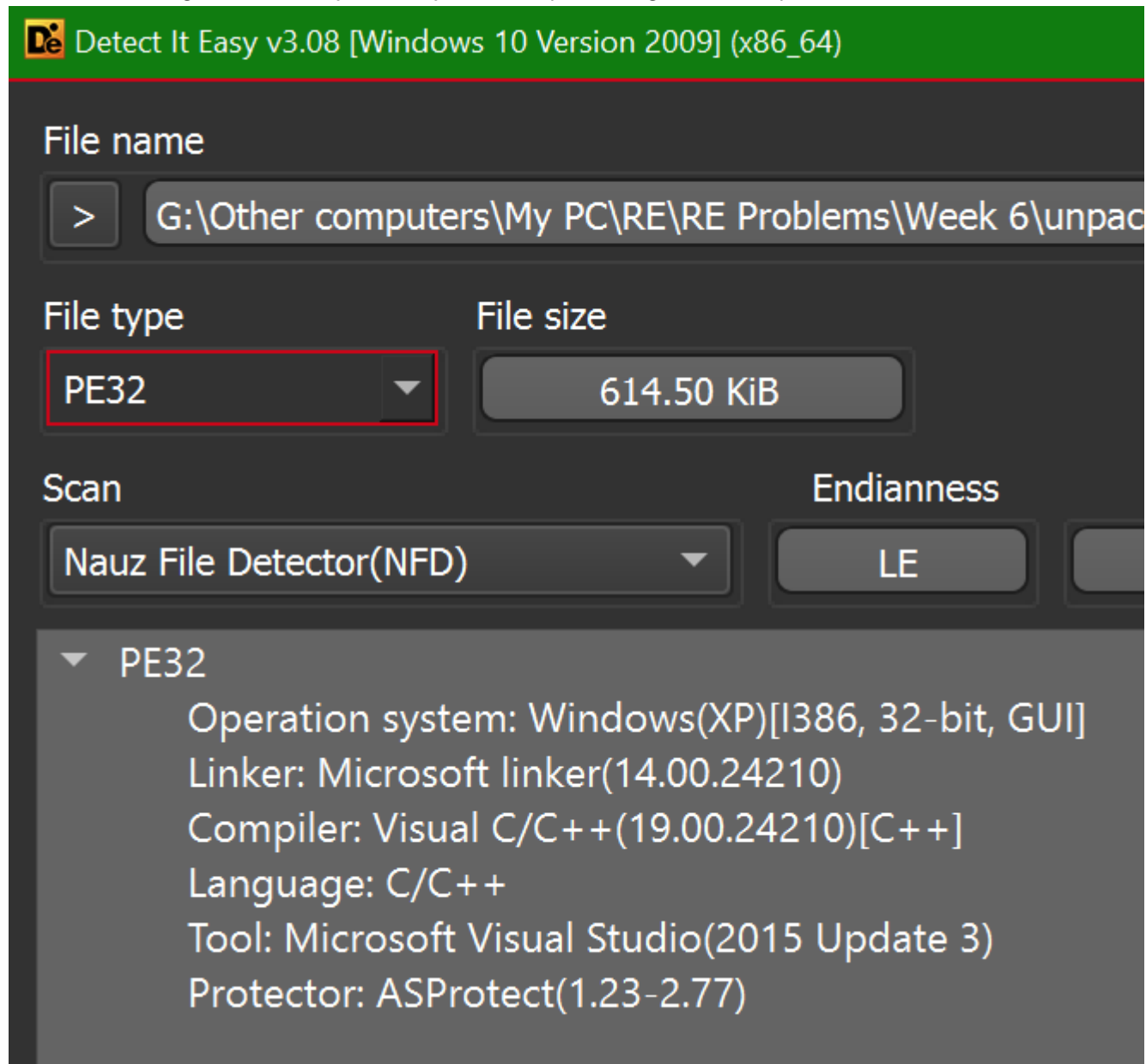


và cut function lỗi còn lại, sau đó dump và fix dump. Kết quả đạt được là file unpack và chạy thành công:



unpackme8\_0E29BE1D445143C4135AA9108DF327C4.exe

Kiểm tra file bằng Detect It Easy cho thấy file được pack bằng ASProtect packer:



Cài OllyDBG Script và dùng script Aspr2.XX\_unpacker\_v1.15E.osc, tìm được OEP:

**CPU - main thread, module unpackme**

| Address  | Hex dump                | ASCII     |
|----------|-------------------------|-----------|
| 00401308 | 88 40 3D 77 00 00 00 00 | @@@=w.... |
| 00401309 | 05 34 91 7C 9C 54 83 7C | 44@!&T\$! |

Registers (FPU)

| Register | Value                      |
|----------|----------------------------|
| EAX      | 00401308 unpackme.00401308 |
| ECX      | 01A100E2                   |
| EDX      | 4F3451E4                   |
| EBX      | 00400000 unpackme.00400000 |
| ESP      | 0012FF68                   |
| EBP      | 0005C82E                   |
| ESI      | 40A7C6E9                   |
| EDI      | 497F2236                   |
| EIP      | 00401308 unpackme.00401308 |

00401597=unpackme.00401597

Dump ra và dùng ImpRec fix IAT, sau đó file chạy thành công:

**Import REConstructor V1.6 Final | MackT/ufCF | YGS-DOX |**

Attach to an Active Process

c:\documents and settings\administrator\desktop\unpackme8\_0e29be1c Pick DLL

Imported Functions Found

- comctl32.dll FT hunk:0000C000 NbFunc:1 (decimal:1) valid:YES
- kernel32.dll FT hunk:0000C008 NbFunc:40 (decimal:64) valid:YES
- user32.dll FT hunk:0000C10C NbFunc:5 (decimal:5) valid:YES
- ? FT hunk:0000C124 NbFunc:1 (decimal:1) valid:NO
- ? FT hunk:0000C12C NbFunc:1 (decimal:1) valid:NO

Log

Current imports:  
 3 (decimal:3) valid module(s)  
 48 (decimal:72) imported function(s) (added: +2 (decimal:2))  
 2 (decimal:2) unresolved pointer(s) (added: +2 (decimal:2))

Show Invalid Options  
 Show Suspect Clear Log  
 Auto Trace About  
 Clear Import Exit

IAT Infos Needed

OEP 00001000  
 IAT AutoSearch  
 RVA 0000C000 Size 00000134