[7] Identify a function that creates a hidden file. In addition, what information does the file contain?

이전에 frida로 추출한 **CreateFile** 행위들 중에서 **dwFlagsAndAttributes가 FILE_ATTRIBUTE_HIDDEN인 파일**을 찾는다. 그리고, 그 파일에 WriteFile을 하는 것도 찾았다.

```
==== CreateFile's lpFileName ====
KU-DFRC-ReverseMe2-Happy-New-Year.hdn
==== CreateFile's dwDesiredAccess ====
0x40000000
==== CreateFile's dwShareMode ====
0x0
==== CreateFile's lpSecurityDisposition ====
NULL
==== CreateFile's dwCreationDisposition ====
0x52002d00000002
==== CreateFile's dwFlagAndAttribution ====
0xc775c72000000002
==== CreateFile's hTemplateFile ====
0x0
```

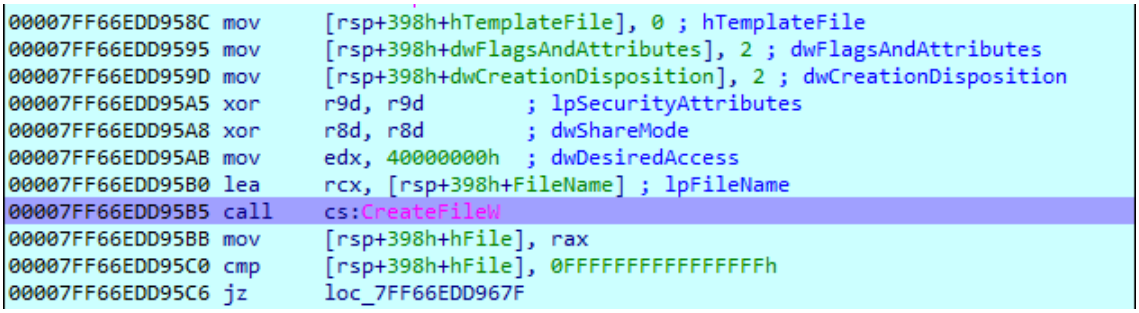
```
==== WriteFile's hFile ====
0x50c
==== WriteFile's lpBuffer ====
Pointer: 0xd1477ff7e0
             0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
d1477ff7e0  31 00 30 00 2e 00 30 00 2e 00 31 00 39 00 30 00  1.0...0...1.9.0.
d1477ff7f0  34 00 33 00 0a 00 44 00 45 00 53 00 4b 00 54 00  4.3...D.E.S.K.T.
d1477ff800  4f 00 50 00 2d 00 41 00 39 00 48 00 52 00 4f 00  O.P.-.A.9.H.R.O.
d1477ff810  41 00 39 00 00 00 00 00 00 00 00 00 00 00 00 00  A.9.............
d1477ff820  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
d1477ff830  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
d1477ff840  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
d1477ff850  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
==== WriteFile's nNumberOfBytesToWrite ====
0x34
==== WriteFile's lpNumberOfBytesWritten ====
Pointer: 0xd1477ff708
             0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
d1477ff708  00 00 00 00 00 00 00 00 4b 00 55 00 2d 00 44 00  ........K.U.-.D.
d1477ff718  46 00 52 00 43 00 2d 00 52 00 65 00 76 00 65 00  F.R.C.-.R.e.v.e.
d1477ff728  72 00 73 00 65 00 4d 00 65 00 32 00 2d 00 48 00  r.s.e.M.e.2.-.H.
d1477ff738  61 00 70 00 70 00 79 00 2d 00 4e 00 65 00 77 00  a.p.p.y.-.N.e.w.
d1477ff748  2d 00 59 00 65 00 61 00 72 00 2e 00 68 00 64 00  -.Y.e.a.r...h.d.
d1477ff758  6e 00 00 00 30 30 30 30 44 00 45 00 53 00 4b 00  n...0000D.E.S.K.
d1477ff768  54 00 4f 00 50 00 2d 00 41 00 39 00 48 00 52 00  T.O.P.-.A.9.H.R.
d1477ff778  4f 00 41 00 39 00 00 00 00 00 00 00 00 00 00 00  O.A.9...........
==== WriteFile's lpOverlapped ====
NULL
```

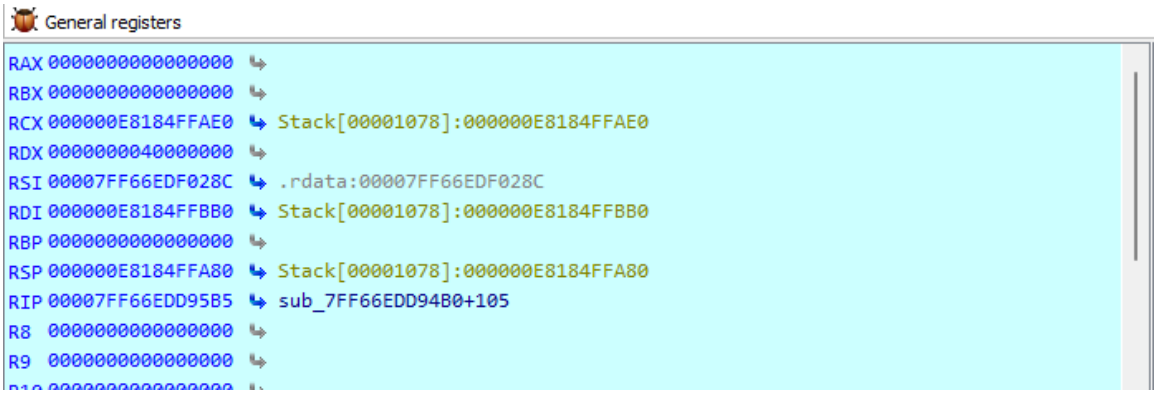
- 따라서 생성된 hidden file은 `KU-DFRC-ReverseMe2-Happy-New-Year.hdn`이다.

1. FUN_1400094b0 CreateFileW

- CreateFileW이 실행되는 함수 중 KU-DFRC-ReverseMe2-Happy-New-Year.hdn 문자열이 있는 함수이다.

- **CreateFileW**이 KU-DFRC-ReverseMe2-Happy-New-Year.hdn을 생성하는게 맞는지 확인하기 위해서 IDA로 중단점을 잡고 디버깅을 해본다.





- rcx가 파일의 이름이므로, 해당 스택을 확인하면 아래와 같고, 이를 Little Endian형식, 아스키 코드로 변환하면 KU-DFRC-ReverseMe2-Happy-New-Year.hdn이 맞다.

```
000000E8184FFAE0  0044002D0055004B
000000E8184FFAE8  002D004300520046
000000E8184FFAF0  0065007600650052
000000E8184FFAF8  004D006500730072
000000E8184FFB00  0048002D00320065
000000E8184FFB08  0079007000700061
000000E8184FFB10  00770065004E002D
000000E8184FFB18  0061006500590020
000000E8184FFB20  00640068002E0072
000000E8184FFB28  000000000000006E
```

- 따라서 이 함수의 **CreateFileW**로 hidden file인 `KU-DFRC-ReverseMe2-Happy-New-Year.hdn`을 생성하였다.

2. FUN_1400094b0 GetComputerNameW, wsprintfW, WriteFile

- **wsprintfW**를 통해서 `local_268`에 어떠한 값을 넣고, 이를 **WriteFile**에 넣이다.
- 하지만 **wsprintW**에 어떤 인자들이 사용되는지 Ghidra에 나와있지 않다. 그래서 인자 4개가 필요하기 때문에 명령어들을 보면서 어떤 인자가 들어있는지 유추했다.

```
          00 fe 7f
1400095f0 48 8d 84        LEA         RAX=>local_2e8,[RSP + 0xb0]
          24 b0 00
          00 00
1400095f8 48 89 44        MOV         qword ptr [RSP + local_370],RAX
          24 28
1400095fd 48 8b 44        MOV         RAX,qword ptr [RSP + local_350]
          24 48
140009602 8b 80 60        MOV         EAX,dword ptr [RAX + offset DAT_7ffe0260]
          02 00 00
140009608 89 44 24 20     MOV         dword ptr [RSP + local_378],EAX
14000960c 48 8b 44        MOV         RAX,qword ptr [RSP + local_350]
          24 48
140009611 44 8b 88        MOV         R9D,dword ptr [RAX + offset DAT_7ffe0270]
          70 02 00 00
140009618 48 8b 44        MOV         RAX,qword ptr [RSP + local_350]
          24 48
14000961d 44 8b 80        MOV         R8D,dword ptr [RAX + offset DAT_7ffe026c]
          6c 02 00 00
140009624 48 8d 15        LEA         RDX,[u_%d.%d.%d_%ws_140020290]
          65 6c 01 00
14000962b 48 8d 8c        LEA         RCX=>local_268,[RSP + 0x130]
          24 30 01
          00 00
140009633 ff 15 b7        CALL        qword ptr [->USER32.DLL::wsprintfW]
          5d 01 00
```

- `"%d.%d.%d\n%ws"` 꼴을 통해서 `"DAT_7ffe026c, DAT_0x7ffe0270, DAT_7ffe0260. local_2e8)` 라고 유추할 수 있었다.

  참고로, `GetComputerNameW(local_2e8, local_358)` 을 통해서 현재 컴퓨터의 정보가 `local_2e8` 에 담아져 있는걸 알고 있다.

- 따라서 **wsprintfW**에 중단점을 걸고 디버깅을 해서 해당 데이터 구간을 확인해보겠다. 데이터 구간은 미리 정해져있는 것 같다.

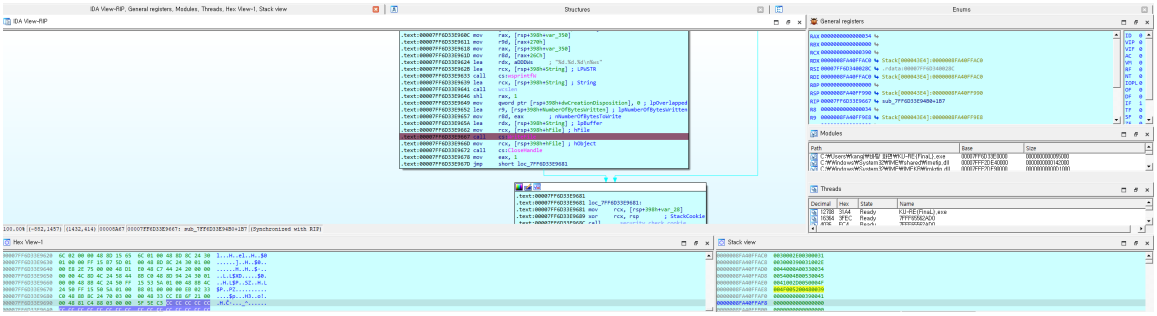
```
000000007FFE0260  00004A63  cJ..
000000007FFE0264  00000001  ....
000000007FFE0268  00090001  ....
000000007FFE026C  0000000A  ....
000000007FFE0270  00000000  ....
```

  - `7ffe026c` : 0A(10)
  - `7ffe0270` : 0
  - `7ffe0260` : 4A63(19043)
  - `local_2e8` : GetComputerName 결과

- 따라서 이 값들을 “%d.%d.%d\n%ws” 형식으로 바꾸면 local_268의 값을 아래와 같다.

```
10.0.19043
"컴퓨터 이름" // 내 컴퓨터에서는 DESKTOP-A9HROA9
```

- **WriteFile**의 **lpbuffer**가 바로 `local_268`이므로, 위의 값이 hidden file에 들어갈 것이다. 확인을 위해 **WriteFileW**에 중단점을 걸고 디버깅을 해본다.



  - 해당 `rdx` 부분을 찾아가보니, frida에서 본것(우리가 예상한 것)과 똑같은 값이 들어가있었다. 따라서 WriteFile을 통해서 해당 데이터를 최종적으로 hidden file에 집어넣었다는 것을 알 수 있다.

Input

```
31 00 30 00 2e 00 30 00 2e 00 31 00 39 00 30 00
34 00 33 00 0a 00 44 00 45 00 53 00 4b 00 54 00
4f 00 50 00 2d 00 41 00 39 00 48 00 52 00 4f 00
41 00 39 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Output

```
1..0.....0.....1..9..0..4..3..
..D..E..S..K..T..O..P..-..A..9..H..R..O..A..9.....................
```

결과

- `KU-DFRC-ReverseMe2-Happy-New-Year.hdn` 이 hidden file이다.
- `FUN_1400094b0`에서 **CreateFile**을 통해 파일을 생성한다. 생성 인자에서 dwFlagsAndAttributes를 0x2(FILE_ATTRIBUTE_HIDDEN)으로 설정해서 hidden file로 생성되는 것이다.
- 또한 `FUN_1400094b0`에서 **WriteFile**을 통해 값을 작성한다. 자세한 부분은 frida에서 확인할 수 있다.
- 파일에 들어있는 데이터는 아래와 같다.

```
10.0.19043              // 파일의 데이터에 있는 값
DESKTOP-A9HROA9         // 내 컴퓨터 이름
```