[6] Explain how and where a file named in “KU-RE{k2y}”is created. In addition, what information does the file contain?

1. KU-RE{k2y} 파일 열기

- frida로 알아본 KU-RE{k2y}의 생성과정이다.

```
==== CreateFile's lpFileName ====
C:\Users\kangj\AppData\Local\Temp\KU-RE{k2y}
==== CreateFile's dwDesiredAccess ====
0x80000000
==== CreateFile's dwShareMode ====
0x1
==== CreateFile's lpSecurityDisposition ====
NULL
==== CreateFile's dwCreationDisposition ====
0x4149444100000003
==== CreateFile's dwFlagAndAttribution ====
0x4151444100000080
==== CreateFile's hTemplateFile ====
0x0
```

- `C:\Users\User\AppData\Local\Temp\KU-RE{k2y}`에 실제로 위치해있는지, Flare-vm에서 확인해보겠다. 숨김파일이어서 보기 옵션을 그에 맞춰서 파일을 찾았다.

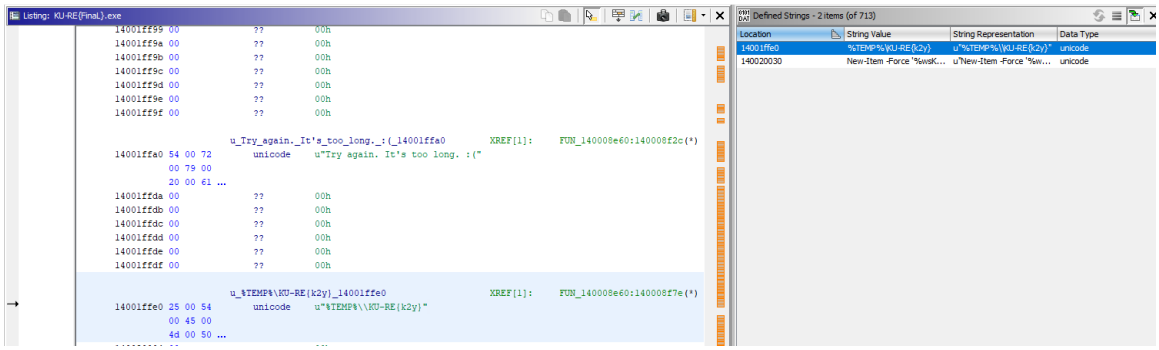
```
4D5A90000300000004000000FFFF0000B8000000000000004000000000000000000000000000000000000000
00000000000000000000000000000000000000100000E1FBA0E00B409CD21B8014CCD21546869732070726F6772
616D2063616E6E6F742062652072756E20696E20444F53206D6F64652E0D0D0A2400000000000000
```

가 파일 안에 들어있는 값이다. 아직 이 값이 뭐를 뜻하는지는 모르겠다. 그런데 4D5A는 어디서 많이 본 값이다…

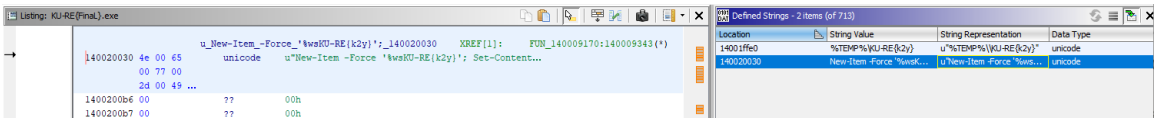
- 4D5A를 아스키로 변환하면 MZ로, 아마도 이게 PE파일의 헤더 부분을 담고 있는게 아닐까...싶다.

2. 파일 생성하는 함수 찾기

- 파일 이름 KU-RE{k2y}가 있는 문자열을 Ghidra에서 찾았다.



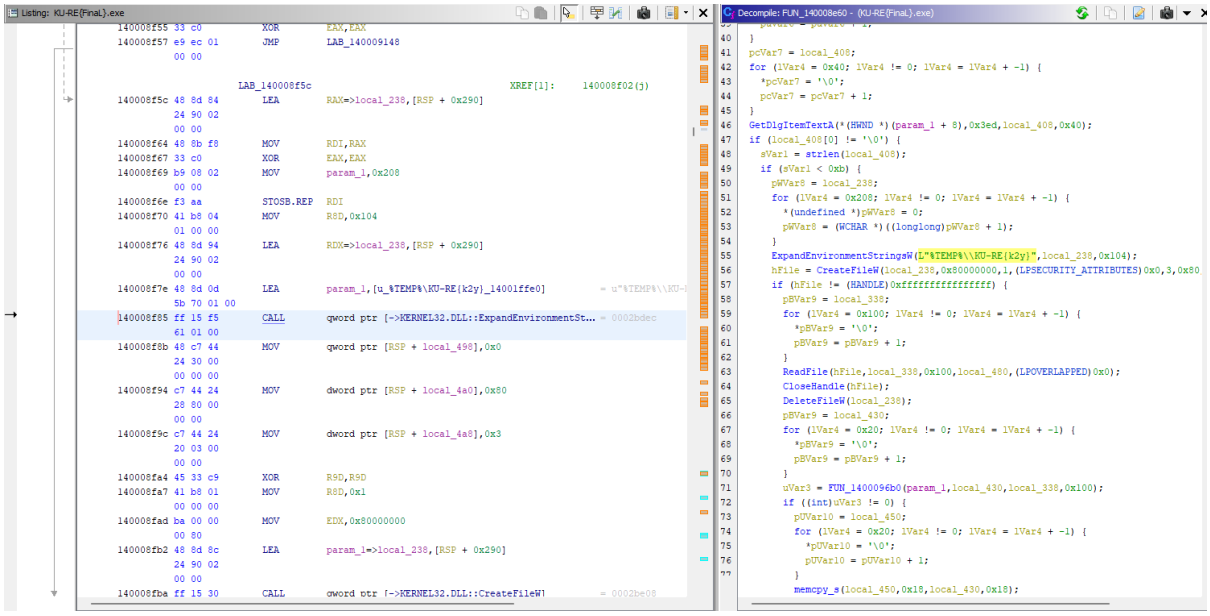
  - 문자열의 XREF는 `FUN_140008e60`이다.



- 문자열의 XREF는 `FUN_140009170`이다.

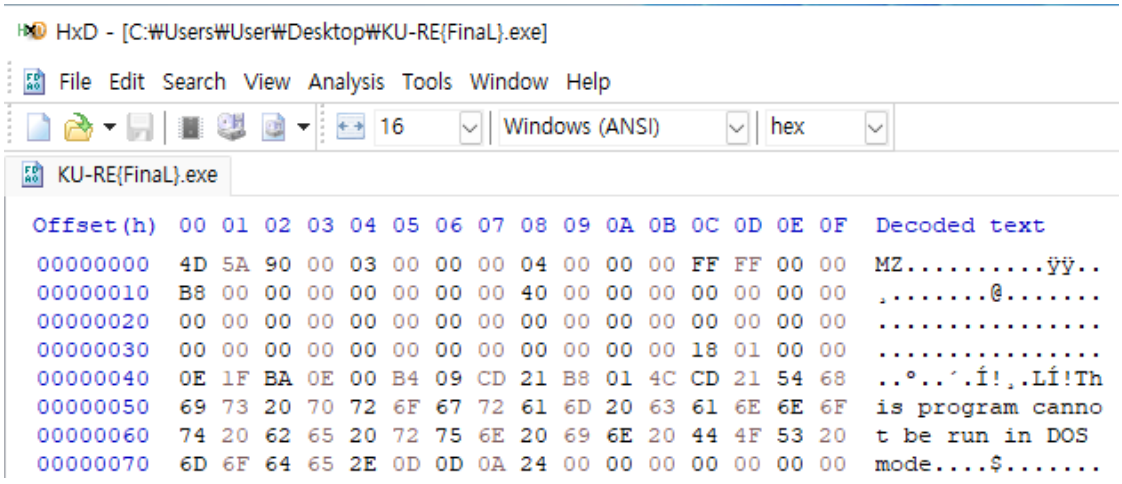
3. FUN_140008e60

- 파일의 이름(경로)이 `local_238`에 담겼으며, 이 이름(경로)으로 **CreateFileW**가 실행됨을 알 수 있다.
- 이 경로로 **KU-RE{k2y}**의 이름을 가진 파일이 생성된다.



4. FUN_140009170

- 맨 처음에 생각했던대로 HxD를 본 결과, 파일에 적힌 데이터는 KU-RE{FinaL}.exe의 앞부분 80바이트였다.



- 그러려면 파일을 열어서 읽어야하므로, 그 함수가 있는 `FUN_140009170`을 찾았다.

```
void FUN_140009170(void)

{
  BOOL BVar1;
  HANDLE hFile;
  LPWSTR _Str;
  size_t sVar2;
  char *_Dst;
  longlong lVar3;
  char *pcVar4;
  byte *pbVar5;
  ushort *puVar6;
  WCHAR *pWVar7;
  char *pcVar8;
  undefined *puVar9;
  undefined auStackY_f08 [32];
  int local_eb8;
  DWORD local_e90 [2];
  _PROCESS_INFORMATION local_e88;
  undefined local_e68 [8];
  undefined local_e60 [104];
  char local_df8 [32];
  undefined local_dd8 [60];
  undefined uStack_d9c;
  byte local_d58 [272];
  WCHAR local_c48 [264];
  ushort local_a38 [264];
  char local_828 [2048];
  ulonglong local_28;

  local_28 = DAT_14002d080 ^ (ulonglong)auStackY_f08;
  puVar9 = local_dd8;
  for (lVar3 = 0x80; lVar3 != 0; lVar3 = lVar3 + -1) {
    *puVar9 = 0;
    puVar9 = puVar9 + 1;
  }
  pbVar5 = local_d58;
  for (lVar3 = 0x101; lVar3 != 0; lVar3 = lVar3 + -1) {
    *pbVar5 = 0;
    pbVar5 = pbVar5 + 1;
  }
  puVar6 = local_a38;
  for (lVar3 = 0x202; lVar3 != 0; lVar3 = lVar3 + -1) {
    *(undefined *)puVar6 = 0;
    puVar6 = (ushort *)((longlong)puVar6 + 1);
  }
  pWVar7 = local_c48;
  for (lVar3 = 0x208; lVar3 != 0; lVar3 = lVar3 + -1) {
    *(undefined *)pWVar7 = 0;
    pWVar7 = (WCHAR *)((longlong)pWVar7 + 1);
  }
  GetModuleFileNameW((HMODULE)0x0,local_c48,0x104);
  hFile = CreateFileW(local_c48,0x80000000,1,(LPSECURITY_ATTRIBUTES)0x0,3,0x80,(HANDLE)0x0);
  if (hFile != (HANDLE)0xffffffffffffffff) {
    BVar1 = ReadFile(hFile,local_dd8,0x80,local_e90,(LPOVERLAPPED)0x0);
    if (BVar1 != 0) {
      uStack_d9c = 0;
      FUN_140009d40((longlong)local_d58,(longlong)local_dd8,0x100);
    }
    CloseHandle(hFile);
    for (local_eb8 = 0; local_eb8 < 0x100; local_eb8 = local_eb8 + 1) {
```

```
      local_a38[local_eb8] = (ushort)local_d58[local_eb8];
    }
    ExpandEnvironmentStringsW(L"%TEMP%\\",local_c48,0x104);
    _Str = (LPWSTR)_calloc_base(0x400,2);
    wsprintfW(_Str,L"New-Item -Force \'%wsKU-RE{k2y}\'; Set-Content \'%wsKU-RE{k2y}\' \'%ws\'");
    pcVar4 = local_828;
    for (lVar3 = 0x800; lVar3 != 0; lVar3 = lVar3 + -1) {
      *pcVar4 = '\0';
      pcVar4 = pcVar4 + 1;
    }
    sVar2 = wcslen(_Str);
    FUN_140001130(local_828,(longlong)_Str,(int)((sVar2 & 0x7fffffff) << 1));
    FUN_14001059c(_Str);
    _Dst = (char *)_calloc_base(0x800,1);
    pcVar4 = "PowerShell.exe -noexit -enc ";
    pcVar8 = local_df8;
    for (lVar3 = 0x1d; lVar3 != 0; lVar3 = lVar3 + -1) {
      *pcVar8 = *pcVar4;
      pcVar4 = pcVar4 + 1;
      pcVar8 = pcVar8 + 1;
    }
    strcat_s(_Dst,0x800,local_df8);
    strcat_s(_Dst,0x800,local_828);
    local_e68._0_4_ = 0x68;
    puVar9 = local_e60;
    for (lVar3 = 0x60; lVar3 != 0; lVar3 = lVar3 + -1) {
      *puVar9 = 0;
      puVar9 = puVar9 + 1;
    }
    BVar1 = CreateProcessA((LPCSTR)0x0,_Dst,(LPSECURITY_ATTRIBUTES)0x0,(LPSECURITY_ATTRIBUTES)0x0,0,
                           0x8000000,(LPVOID)0x0,(LPCSTR)0x0,(LPSTARTUPINFOA)local_e68,&local_e88);
    if (BVar1 != 0) {
      CloseHandle(local_e88.hProcess);
      CloseHandle(local_e88.hThread);
    }
    FUN_14001059c(_Dst);
  }
  FUN_14000b800(local_28 ^ (ulonglong)auStackY_f08);
  return;
}
```

- **GetModuleFileNameW**로 현재 실행시키는 파일의 이름과 경로가 `local_c48`에 담긴다.

  해당 경로로 **CreateFileW**를 실행해 현재 실행파일을 열어 `hFile`에 담는다. (왜냐하면 `dwCreationDisposition=3`)

  ```
  GetModuleFileNameW((HMODULE)0x0,local_c48,0x104);
  hFile = CreateFileW(local_c48,0x80000000,1,(LPSECURITY_ATTRIBUTES)0x0,3,0x80,(HANDLE)0x0);
  ```

- ReadFile로 현재 실행파일(KU-RE{FinaL}.exe)의 0x80바이트를 읽어서 `local_dd8`에 저장한다.

```
BVar1 = ReadFile(hFile,local_dd8,0x80,local_e90,(LPOVERLAPPED)0x0);
```

- 이 방법으로 KU-RE{k2y}에 넣을 데이터값을 얻어냈다.

결과

- 저장 위치: `C:\Users\User\AppData\Local\Temp\KU-RE{k2y}`
- `FUN_140008e60`에서 실행되는 **CreateFileW**로 인해, 생성된다.
- KU-RE{FinaL}.exe의 맨 앞 80바이트(DOS HEADER와 문구)를 담고 있다.