Tue 10:30
Thur 10:30

Robot #301

역공학

Reverse Engineering

Crafting Your Own PE File

Assignment #1

박 정 흠

Park, Jungheum

jungheumpark@korea.ac.kr

Korea University
School of Cybersecurity

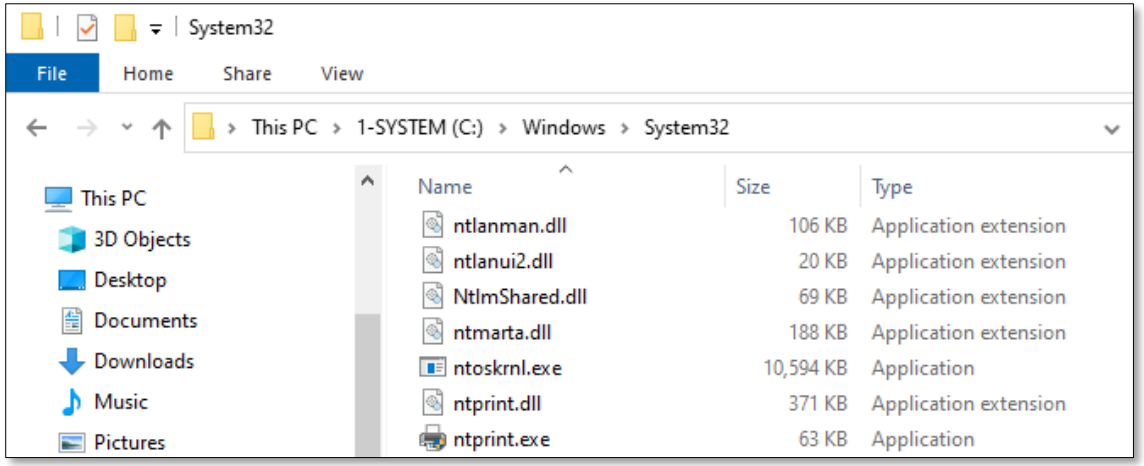
Crafting Your Own PE File

Crafting Your Own PE File

Source Codes

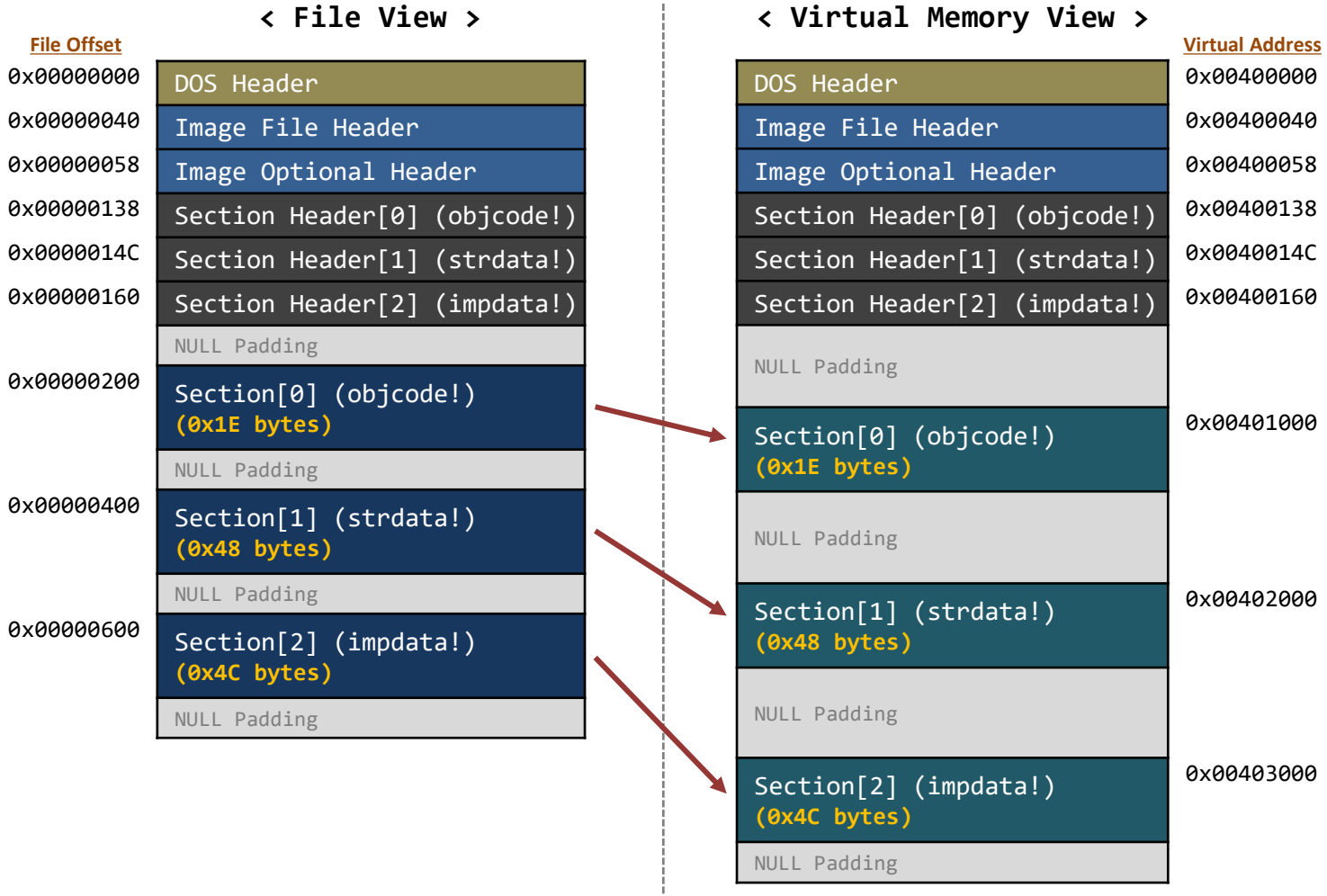
```
#include <Windows.h>
#include <tchar.h>

void main(int argc, char *argv[])
{
    ShellExecuteW(NULL, _T("open"), _T("explorer"), _T("c:\\windows\\system32"), NULL, SW_SHOWNORMAL);
}
```

- **Additional Information**
  - ShellExecuteW (SHELL32.dll)
  - NULL: 0x00
  - SW_SHOWNORMAL: 0x01
  - _T(“string”): Unicode



Crafting Your Own PE File

Internal Structure



File Alignment
Unit = 0x200 (512)

Section Alignment
Unit = 0x1000 (4,096)

Crafting Your Own PE File

DOS Header

- **Generating DOS Header**

```
typedef struct _IMAGE_DOS_HEADER {
        WORD  e_magic;     // 00: 'MZ' Header signature
        … …                // 58 (0x3A) bytes
        DWORD e_lfanew;    // 3c: Offset to extended header */
} IMAGE_DOS_HEADER, *PIMAGE_DOS_HEADER;
```

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  4D 5A 00 00 00 00 00 00 00 00 00 00 00 00 00 00  MZ..............
00000010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00  ............@...
```

- DOS Stub can be omitted

Crafting Your Own PE File

NT Header - Signature + Image File Header

- **NT Header Signature (4):** `0x50450000 ('PE'00)`

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  4D 5A 00 00 00 00 00 00 00 00 00 00 00 00 00 00  MZ..............
00000010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00  ............@...
00000040  50 45 00 00 4C 01 03 00 00 00 00 00 00 00 00 00  PE..L...........
00000050  00 00 00 00 E0 00 02 01                          ....à...
```

- **IMAGE_FILE_HEADER (20 bytes)**
  - **Machine (2):** `0x014C (IMAGE_FILE_MACHINE_I386)`
  - **NumberOfSections (2):** `0x0003`
  - **TimeDateStamp (4):** `0x00000000`
  - **SizeOfOptionalHeader (2):** `0x00E0`
  - **Characteristics (2):** `0x0102`
    - `#define IMAGE_FILE_EXECUTABLE_IMAGE 0x0002 // File is executable`
    - `#define IMAGE_FILE_32BIT_MACHINE 0x0100 // 32-bit machine`

Crafting Your Own PE File

NT Header - Image Optional Header

- **IMAGE_OPTIONAL_HEADER (224 bytes)**

```
WORD    Magic;                                          0x010B     (32 bits)
BYTE    MajorLinkerVersion, MinorLinkerVersion;         0x00
DWORD   SizeOfCode;                                     0x00000200 (objcode!)
DWORD   SizeOfInitialzedData, SizeOfUnintializedData;   0x00000000
DWORD   AddressOfEntryPoint;                            0x00001000 (objcode!)
DWORD   BaseOfCode;                                     0x00001000 (objcode!)
DWORD   BaseOfData;                                     0x00002000 (strdata!)
DWORD   ImageBase;                                      0x00400000
DWORD   SectionAlignment;                               0x00001000
DWORD   FileAlignment;                                  0x00000200
WORD    MajorOperatingSystemVersion ~ MinorImageVersion; 0x0000
WORD    MajorSubsystemVersion;                          0x0006      (Windows Vista+)
WORD    MinorSubsystemVersion;                          0x0000
DWORD   Win32VersionValue;                              0x00000000
DWORD   SizeOfImage;                                    0x00004000
DWORD   SizeOfHeaders;                                  0x00000200
DWORD   Checksum;                                       0x00000000
WORD    Subsystem;                                      0x0002      (Windows GUI)
WORD    DllCharacteristics;                             0x0000
DWORD   SizeOfStackReserve, SizeOfHeapReserve;          0x00010000
DWORD   SizeOfStackCommit, SizeOfHeapCommit;            0x00001000
DWORD   LoaderFlags;                                    0x00000000
DWORD   NumberOfRvaAndSizes;                            0x00000010
```

Crafting Your Own PE File

NT Header - Image Optional Header

- **IMAGE_OPTIONAL_HEADER (224 bytes)**

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	4D	5A	00	00	00	00	00	00	00	00	00	00	00	00	00	00	MZ.....
00000010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	40	00	00	00	.....@...
00000040	50	45	00	00	4C	01	03	00	00	00	00	00	00	00	00	00	PE..L.....
00000050	00	00	00	00	E0	00	02	01	0B	01	00	00	00	02	00	00	....à.....
00000060	00	00	00	00	00	00	00	00	00	10	00	00	00	10	00	00	.....
00000070	00	20	00	00	00	00	40	00	00	10	00	00	00	02	00	00	. ....@.....
00000080	00	00	00	00	00	00	00	00	06	00	00	00	00	00	00	00	.....
00000090	00	40	00	00	00	02	00	00	00	00	00	00	02	00	00	00	.@.....
000000A0	00	00	01	00	00	10	00	00	00	00	01	00	00	10	00	00	.....
000000B0	00	00	00	00	10	00	00	00									.....

Crafting Your Own PE File

NT Header - Image Optional Header

- **IMAGE_OPTIONAL_HEADER: DataDirectory[0] ~ DataDirectory[15]**
  - 8 bytes x 16 Entry = 128 (0x80) bytes

```
typedef struct _IMAGE_DATA_DIRECTORY {

        DWORD VirtualAddress;
        DWORD Size;

} IMAGE_DATA_DIRECTORY, *PIMAGE_DATA_DIRECTORY;
```

```
000000A0  00 00 01 00 00 10 00 00 00 00 01 00 00 10 00 00  ................
000000B0  00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00  ................
000000C0  00 30 00 00 28 00 00 00 00 00 00 00 00 00 00 00  .0..(...........
000000D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000130  00 00 00 00 00 00 00 00                          ........
```

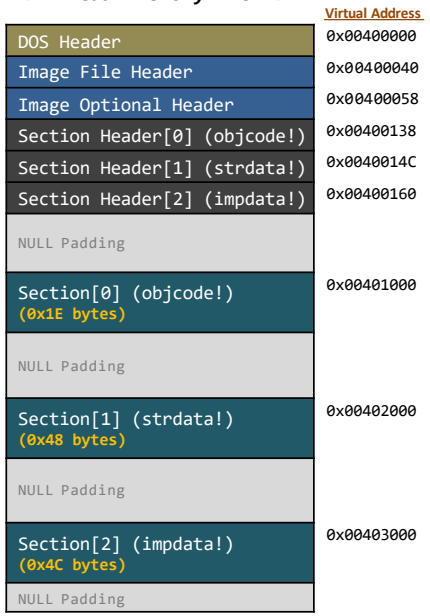
Crafting Your Own PE File

NT Header - Image Optional Header

- **IMAGE_OPTIONAL_HEADER: DataDirectory[0] ~ DataDirectory[15]**
  - DataDirectory[1] = IMAGE_DIRECTORY_ENTRY_**IMPORT**
    - VirtualAddress (4): 0x00003000
    - Size (4): 0x00000028 (40 bytes)
      - Why 40 bytes? `IMAGE_IMPORT_DESCRIPTOR` = 20 bytes

```
000000A0  00 00 01 00 00 10 00 00 00 00 01 00 00 10 00 00  ................
000000B0  00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00  ................
000000C0  00 30 00 00 28 00 00 00 00 00 00 00 00 00 00 00  .0..(...........
000000D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000130  00 00 00 00 00 00 00 00                          ........
```

< Virtual Memory View >



Crafting Your Own PE File

Section Header - objcode! Section

```
00000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000130  00 00 00 00 00 00 00 00 6F 62 6A 63 6F 64 65 21  ........objcode!
00000140  1E 00 00 00 00 10 00 00 00 02 00 00 00 02 00 00  ................
00000150  00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60  ............ ..`
```

- **Name** (8): objcode!
- **VirtualSize** (4): 0x0000001E
- **VirtualAddress** (4): 0x00001000
- **SizeOfRawData** (4): 0x00000200
- **PointerToRawData** (4): 0x00000200

- **Characteristics (4): 0x60000020**
  - IMAGE_SCN_CNT_CODE 0x00000020
  - IMAGE_SCN_MEM_EXECUTE 0x20000000
  - IMAGE_SCN_MEM_READ 0x40000000

Crafting Your Own PE File

Section Header - strdata! Section

```
00000130  00 00 00 00 00 00 00 00 6F 62 6A 63 6F 64 65 21  ........objcode!
00000140  1E 00 00 00 00 10 00 00 00 02 00 00 00 02 00 00  ................
00000150  00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60  ............ ..`
00000160  73 74 72 64 61 74 61 21 48 00 00 00 00 20 00 00  strdata!H.... ..
00000170  00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00  ................
00000180  00 00 00 00 40 00 00 C0                          ....@..À
```

- **Name** (8): strdata!
- **VirtualSize** (4): 0x00000048
- **VirtualAddress** (4): 0x00002000
- **SizeOfRawData** (4): 0x00000200
- **PointerToRawData** (4): 0x00000400
- **Characteristics** (4): 0xC0000040
  - IMAGE_SCN_INITIALIZED_DATA 0x00000040
  - IMAGE_SCN_MEM_READ 0x40000000
  - IMAGE_SCN_MEM_WRITE 0x80000000

Crafting Your Own PE File

Section Header - impdata! Section

```
00000130  00 00 00 00 00 00 00 00 6F 62 6A 63 6F 64 65 21  ........objcode!
00000140  1E 00 00 00 00 10 00 00 00 02 00 00 00 02 00 00  ................
00000150  00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60  ............ ..`
00000160  73 74 72 64 61 74 61 21 48 00 00 00 00 20 00 00  strdata!H.... ..
00000170  00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00  ................
00000180  00 00 00 00 40 00 00 C0 69 6D 70 64 61 74 61 21  ....@..Àimpdata!
00000190  4C 00 00 00 00 30 00 00 00 02 00 00 00 06 00 00  L....0..........
000001A0  00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40  ............@..@
```

- **Name** (8): impdata!
- **VirtualSize** (4): 0x0000004C
- **VirtualAddress** (4): 0x00003000
- **SizeOfRawData** (4): 0x00000200
- **PointerToRawData** (4): 0x00000600

- **Characteristics (4):** 0x40000040
  - IMAGE_SCN_INITIALIZED_DATA 0x00000040
  - IMAGE_SCN_MEM_READ 0x40000000

Crafting Your Own PE File

[REF] Gap between Header and Body

- **Add Padding (0x00) bytes**

```
00000130  00 00 00 00 00 00 00 00 6F 62 6A 63 6F 64 65 21  ........objcode!
00000140  1E 00 00 00 00 10 00 00 00 02 00 00 00 02 00 00  ................
00000150  00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60  ............ ..`
00000160  73 74 72 64 61 74 61 21 48 00 00 00 00 20 00 00  strdata!H.... ..
00000170  00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00  ................
00000180  00 00 00 00 40 00 00 C0 69 6D 70 64 61 74 61 21  ....@..Àimpdata!
00000190  4C 00 00 00 00 30 00 00 00 02 00 00 00 06 00 00  L....0..........
000001A0  00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40  ............@..@
000001B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

- FileAlignment: 0x200 (512) bytes

Crafting Your Own PE File

Section Data - strdata! Section

```
void main(int argc, char *argv[])
{
    ShellExecuteW(NULL, _T("open"), _T("explorer"), _T("c:\\windows\\system32"), NULL, SW_SHOWNORMAL);
}
```

RVA																	
	000003E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
	000003F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0x2000	00000400	6F	00	70	00	65	00	6E	00	00	00	00	00	65	00	78	00	o.p.e.n.....e.x.
0x2010	00000410	70	00	6C	00	6F	00	72	00	65	00	72	00	00	00	00	00	p.l.o.r.e.r.....
0x2020	00000420	63	00	3A	00	5C	00	77	00	69	00	6E	00	64	00	6F	00	c.:.\.w.i.n.d.o.
0x2030	00000430	77	00	73	00	5C	00	73	00	79	00	73	00	74	00	65	00	w.s.\.s.y.s.t.e.
0x2040	00000440	6D	00	33	00	32	00	00	00	00	00	00	00	00	00	00	00	m.3.2.....
	00000450	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
	00000460	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

- _T("open")
  - 0x00402000 (VA) = 0x00400000 (ImageBase) + 0x00002000 (RVA of strdata!) + 0x00
- _T("explorer")
  - 0x0040200C (VA) = 0x00400000 (ImageBase) + 0x00002000 (RVA of strdata!) + 0x0C
- _T("c:\\Windows\\System32")
  - 0x00402020 (VA) = 0x00400000 (ImageBase) + 0x00002000 (RVA of strdata!) + 0x20

Crafting Your Own PE File

Section Data - impdata! Section

```
000005F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000600  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000610  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000620  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000630  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000640  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000650  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

(1) (2) (3) (4) (5)

- (1) `IMAGE_IMPORT_DESCRIPTOR[0]`
- (2) `IMAGE_IMPORT_DESCRIPTOR[1]` = `NULL`
- (3) INT (Image Name Table) & IAT (Image Address Table) address list
- (4) `IMAGE_IMPORT_BY_NAME`
- (5) DLL name

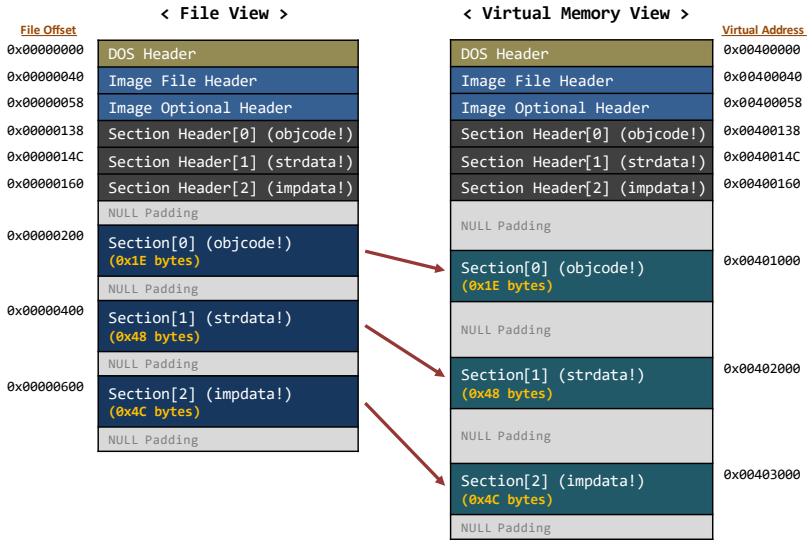
Crafting Your Own PE File

Section Data - impdata! Section

- **IMAGE_IMPORT_DESCRIPTOR**

RVA																	
	000005F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0x3000	00000600	28	30	00	00	00	00	00	00	00	00	00	00	40	30	00	00	(0.....@0..
0x3010	00000610	28	30	00	00	00	00	00	00	00	00	00	00	00	00	00	00	(0.....
0x3020	00000620	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0x3030	00000630	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0x3040	00000640	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
	00000650	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

- `OriginalFirstThunk (4): 0x00003028 // INT address list`
- `TimeDateStamp (4): 0x00000000 // unbounded`
- `ForwarderChain (4): 0x00000000`
- `Name (4): 0x00003040`
- `FirstThunk (4): 0x00003028 // IAT address list`



Crafting Your Own PE File

Section Data - impdata! Section

- **INT (Image Name Table) & IAT (Image Address Table) Address List**

RVA																	
	000005F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0x3000	00000600	28	30	00	00	00	00	00	00	00	00	00	00	40	30	00	00	(0.....@0..
0x3010	00000610	28	30	00	00	00	00	00	00	00	00	00	00	00	00	00	00	(0.....
0x3020	00000620	00	00	00	00	00	00	00	00	30	30	00	00	00	00	00	00	.....00.....
0x3030	00000630	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0x3040	00000640	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
	00000650	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

- There is only one imported function
- At 0x00003028 (RVA), set an RVA (0x00003030) where IMAGE_IMPORT_BY_NAME is located
  - Note that OriginalFirstThunk & FirstThunk have the same value ‘0x00003028’

Crafting Your Own PE File

Section Data - impdata! Section

- **IMAGE_IMPORT_BY_NAME**

RVA																	
	000005F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0x3000	00000600	28	30	00	00	00	00	00	00	00	00	00	00	40	30	00	00	(0.....@0..
0x3010	00000610	28	30	00	00	00	00	00	00	00	00	00	00	00	00	00	00	(0.....
0x3020	00000620	00	00	00	00	00	00	00	00	30	30	00	00	00	00	00	00	.....00.....
0x3030	00000630	00	00	53	68	65	6C	6C	45	78	65	63	75	74	65	57	00	..ShellExecuteW.
0x3040	00000640	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
	00000650	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

- An imported function's information is stored at 0x00003030 (RVA)
  - Hint: NULL
  - Name: "ShellExecuteW"

Crafting Your Own PE File

Section Data - impdata! Section

- **DLL Name**

RVA																	
	000005F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0x3000	00000600	28	30	00	00	00	00	00	00	00	00	00	00	40	30	00	00	(0.....@0..
0x3010	00000610	28	30	00	00	00	00	00	00	00	00	00	00	00	00	00	00	(0.....
0x3020	00000620	00	00	00	00	00	00	00	00	30	30	00	00	00	00	00	00	.....00.....
0x3030	00000630	00	00	53	68	65	6C	6C	45	78	65	63	75	74	65	57	00	..ShellExecuteW.
0x3040	00000640	53	48	45	4C	4C	33	32	2E	64	6C	6C	00	00	00	00	00	SHELL32.dll.....
	00000650	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

- DLL name (SHELL32.dll) is stored at 0x00003040 (RVA)

Crafting Your Own PE File

Section Data - objcode! Section

```
void main(int argc, char *argv[])
{
    ShellExecuteW(NULL, _T("open"), _T("explorer"), _T("c:\\windows\\system32"), NULL, SW_SHOWNORMAL);
}
```

```
401000    6A 01          PUSH 1              ; IsShown = 1
401002    6A 00          PUSH 0              ; DefDir = NULL
401004    68 20204000    PUSH 0x00402020     ; Parameters = "c:\windows\system32"
401009    68 0C204000    PUSH 0x0040200C     ; FileName = "explorer"
40100E    68 00204000    PUSH 0x00402000     ; Operation = "open"
401013    6A 00          PUSH 0              ; hWnd = NULL
401015    FF15 28304000  CALL [0x00403028]   ; ShellExecuteW
40101B    33C0           XOR EAX,EAX
40101D    C3             RETN
```

```
      000003E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
RVA   000003F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x2000 00000400  6F 00 70 00 65 00 6E 00 00 00 00 00 65 00 78 00  o.p.e.n.....e.x.
0x2010 00000410  70 00 6C 00 6F 00 72 00 65 00 72 00 00 00 00 00  p.l.o.r.e.r.....
0x2020 00000420  63 00 3A 00 5C 00 77 00 69 00 6E 00 64 00 6F 00  c.:.\.w.i.n.d.o.
0x2030 00000430  77 00 73 00 5C 00 73 00 79 00 73 00 74 00 65 00  w.s.\.s.y.s.t.e.
0x2040 00000440  6D 00 33 00 32 00 00 00 00 00 00 00 00 00 00 00  m.3.2...........
       00000450  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
       00000460  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
RVA   000005F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x3000 00000600  28 30 00 00 00 00 00 00 00 00 00 00 40 30 00 00  (0..........@0..
0x3010 00000610  28 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00  (0..............
0x3020 00000620  00 00 00 00 00 00 00 00 30 30 00 00 00 00 00 00  ........00......
0x3030 00000630  00 00 53 68 65 6C 6C 45 78 65 63 75 74 65 57 00  ..ShellExecuteW.
0x3040 00000640  53 48 45 4C 4C 33 32 2E 64 6C 6C 00 00 00 00 00  SHELL32.dll.....
       00000650  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
000001E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000200  6A 01 6A 00 68 20 20 40 00 68 0C 20 40 00 68 00  j.j.h  @.h. @.h.
00000210  20 40 00 6A 00 FF 15 28 30 40 00 33 C0 C3 00 00   @.j.ÿ.(0@.3ÀÃ..
00000220  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000230  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

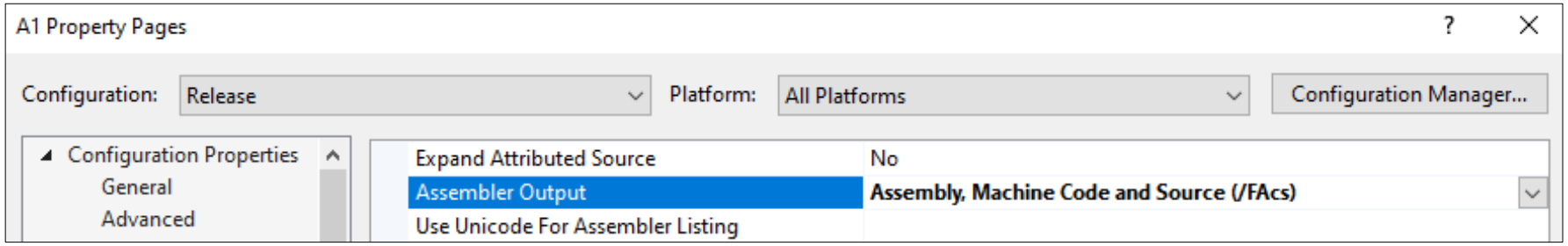
- CALL [0x00403028] ?
  - IAT's addresses will be replaced by PE loader

Address	Hex				ASCII
00403000	28 30 00 00	00 00 00 00	00 00 00 00	40 30 00 00	(0.....@0..
00403010	28 30 00 00	00 00 00 00	00 00 00 00	00 00 00 00	(0.....
00403020	00 00 00 00	00 00 00 00	70 37 E1 75	00 00 00 00	.....p7áu....
00403030	00 00 53 68	65 6C 6C 45	78 65 63 75	74 65 57 00	..ShellExecuteW.
00403040	53 48 45 4C	4C 33 32 2E	64 6C 6C 00	00 00 00 00	SHELL32.dll.....

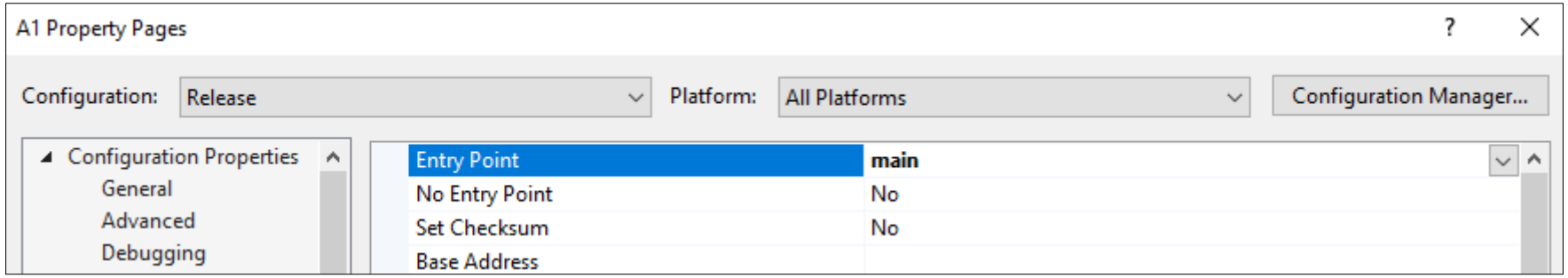
Crafting Your Own PE File

[REF] Visual Studio's Options

- **Generating Assembly and Machine Codes**
  - C/C++ → Output Files → Assembler Output



- **Excluding Startup Codes**
  - Linker → Advanced → Entry Point



Crafting Your Own PE File

Inspecting PE File

PPEE - C:\Users\User\Desktop\samples\re\jpark\A1.exe

File Plugins Help

- DOS Header
- NT Header
  - File Header
  - Optional Header
    - Data Directories
- Section Headers
- DIRECTORY_ENTRY_IMPORT
- Strings in file
  - ASCII
  - UNICODE
  - URL
  - Registry
  - Suspicious

Member	Value	Comment
Magic	010B	PE32
MajorLinkerVersion	00	
MinorLinkerVersion	00	
SizeOfCode	00000200	
SizeOfInitializedData	00000000	
SizeOfUninitializedData	00000000	
AddressOfEntryPoint	00001000	objcode!
BaseOfCode	00001000	
BaseOfData	00002000	
ImageBase	00400000	
SectionAlignment	00001000	
FileAlignment	00000200	
MajorOperatingSystemVersion	0000	
MinorOperatingSystemVersion	0000	
MajorImageVersion	0000	
MinorImageVersion	0000	
MajorSubsystemVersion	0006	
MinorSubsystemVersion	0000	
Win32VersionValue	00000000	
SizeOfImage	00004000	
SizeOfHeaders	00000200	
CheckSum	00000000	Correct: 0001061D
Subsystem	0002	Windows GUI
DllCharacteristics	0000	
SizeOfStackReserve	00010000	
SizeOfStackCommit	00001000	
SizeOfHeapReserve	00010000	
SizeOfHeapCommit	00001000	
LoaderFlags	00000000	
NumberOfRvaAndSizes	00000010	

PEview - C:\Users\User\Desktop\samples\re\jpark\A1.exe

File View Go Help

- A1.exe
  - IMAGE_DOS_HEADER
  - MS-DOS Stub Program
  - IMAGE_NT_HEADERS
  - IMAGE_SECTION_HEADER objcode!
  - IMAGE_SECTION_HEADER strdata!
  - IMAGE_SECTION_HEADER impdata!
  - SECTION objcode!
  - SECTION strdata!
  - SECTION impdata!
    - IMPORT Directory Table

pFile	Raw Data	Value
00000200	6A 01 6A 00 68 20 20 40 00 68 0C 20 40 00 68 00	j.j.h @.h. @.h.
00000210	20 40 00 6A 00 FF 15 28 30 40 00 33 C0 C3 00 00	@.j...(0@.3....
00000220	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000230	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000240	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000250	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000260	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000270	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000280	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000290	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

PEview - C:\Users\User\Desktop\samples\re\jpark\A1.exe

File View Go Help

- A1.exe
  - IMAGE_DOS_HEADER
  - MS-DOS Stub Program
  - IMAGE_NT_HEADERS
  - IMAGE_SECTION_HEADER objcode!
  - IMAGE_SECTION_HEADER strdata!
  - IMAGE_SECTION_HEADER impdata!
  - SECTION objcode!
  - SECTION strdata!
  - SECTION impdata!
    - IMPORT Directory Table

pFile	Raw Data	Value
00000400	6F 00 70 00 65 00 6E 00 00 00 00 00 65 00 78 00	o.p.e.n.....e.x.
00000410	70 00 6C 00 6F 00 72 00 65 00 72 00 00 00 00 00	p.l.o.r.e.r.....
00000420	63 00 3A 00 5C 00 77 00 69 00 6E 00 64 00 6F 00	c.:.\.w.i.n.d.o.
00000430	77 00 73 00 5C 00 73 00 79 00 73 00 74 00 65 00	w.s.\.s.y.s.t.e.
00000440	6D 00 33 00 32 00 00 00 00 00 00 00 00 00 00 00	m.3.2.....
00000450	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000460	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000470	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000480	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000490	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

PEview - C:\Users\User\Desktop\samples\re\jpark\A1.exe

File View Go Help

- A1.exe
  - IMAGE_DOS_HEADER
  - MS-DOS Stub Program
  - IMAGE_NT_HEADERS
  - IMAGE_SECTION_HEADER objcode!
  - IMAGE_SECTION_HEADER strdata!
  - IMAGE_SECTION_HEADER impdata!
  - SECTION objcode!
  - SECTION strdata!
  - SECTION impdata!
    - IMPORT Directory Table

pFile	Raw Data	Value
00000600	28 30 00 00 00 00 00 00 00 00 00 00 40 30 00 00	(0.....@0..
00000610	28 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00	(0.....
00000620	00 00 00 00 00 00 00 00 30 30 00 00 00 00 00 00	.....00.....
00000630	00 00 53 68 65 6C 6C 45 78 65 63 75 74 65 57 00	..ShellExecuteW.
00000640	53 48 45 4C 4C 33 32 2E 64 6C 6C 00 00 00 00 00	SHELL32.dll.....
00000650	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000660	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000670	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000680	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000690	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

What You Must Do

What You Must Do

Crafting Your Own 32-bit PE File

- **Your PE File Must**
  - Call MessageBoxW function
  - Print your “Student ID” and “Full name” as shown in the right screenshot

- **Conditions**
  - At least three sections
    - You can freely set section names
      - e.g., codes (‘code’), strings (‘sdata’), imports (‘idata’)
  - Order of sections
    - Student ID ending with **odd** number: **strings** → **codes** → **imports**
    - Student ID ending with **even** number: **strings** → **imports** → **codes**

What You Must Do

[REF] Creating the Smallest Possible PE Executable

- http://www.phreedom.org/research/tinype/

- **Smallest possible PE file**
  - 97 bytes

- **Smallest possible PE file on Windows 2000**
  - 133 bytes

```
opthdr:
    dw 0x10B                        ; Magic (PE32)
    db 8                            ; MajorLinkerVersion UNUSED
    db 0                            ; MinorLinkerVersion UNUSED
    dd round(codesize, filealign)   ; SizeOfCode UNUSED
    dd 0                            ; SizeOfInitializedData UNUSED
    dd 0                            ; SizeOfUninitializedData UNUSED
    dd start                        ; AddressOfEntryPoint
    dd code                         ; BaseOfCode UNUSED
    dd round(filesize, sectalign)   ; BaseOfData UNUSED
    dd 0x400000                     ; ImageBase
    dd sectalign                    ; SectionAlignment
    dd filealign                    ; FileAlignment
    dw 4                            ; MajorOperatingSystemVersion UNUSED
    dw 0                            ; MinorOperatingSystemVersion UNUSED
    dw 0                            ; MajorImageVersion UNUSED
    dw 0                            ; MinorImageVersion UNUSED
    dw 4                            ; MajorSubsystemVersion
    dw 0                            ; MinorSubsystemVersion UNUSED
    dd 0                            ; Win32VersionValue UNUSED
    dd round(filesize, sectalign)   ; SizeOfImage
    dd round(hdrsize, filealign)    ; SizeOfHeaders
    dd 0                            ; CheckSum UNUSED
    dw 2                            ; Subsystem (Win32 GUI)
    dw 0x400                        ; DllCharacteristics UNUSED
    dd 0x100000                     ; SizeOfStackReserve UNUSED
    dd 0x1000                       ; SizeOfStackCommit
    dd 0x100000                     ; SizeOfHeapReserve
    dd 0x1000                       ; SizeOfHeapCommit UNUSED
    dd 0                            ; LoaderFlags UNUSED
    dd 16                           ; NumberOfRvaAndSizes UNUSED
```

How to Submit

How to Submit

Documentation Rules

- **Write a Technical Report using Markdown**
  - You should explain your step-by-step processes
  - Report structure
    - For this assignment, you can freely design your own report
  - [REF] Apps/Services for writing Markdown files:
    - You can choose anyone such as *VS Code*, *R*, *Typora*, *Notion* …
      - Syntax: https://support.typora.io/Markdown-Reference

How to Submit

Submission Rules

- **Submit Your Files to the Blackboard** (‘Assignments and Tests’ page)
  - File format: ZIP
    - Executable file (EXE) + Report file (PDF)
  - File name: [2022-RE]-[*ID*]-[*NAME*]

- **Deadline**
  - 2022.10.06. (Thur) 10:29

- **Points**
  - Binary (4), Report (6)

THANK YOU
for Listening!

jungheumpark@korea.ac.kr

KOREA UNIVERSITY Digital Forensic Research Center | dfrc.korea.ac.kr

Questions?