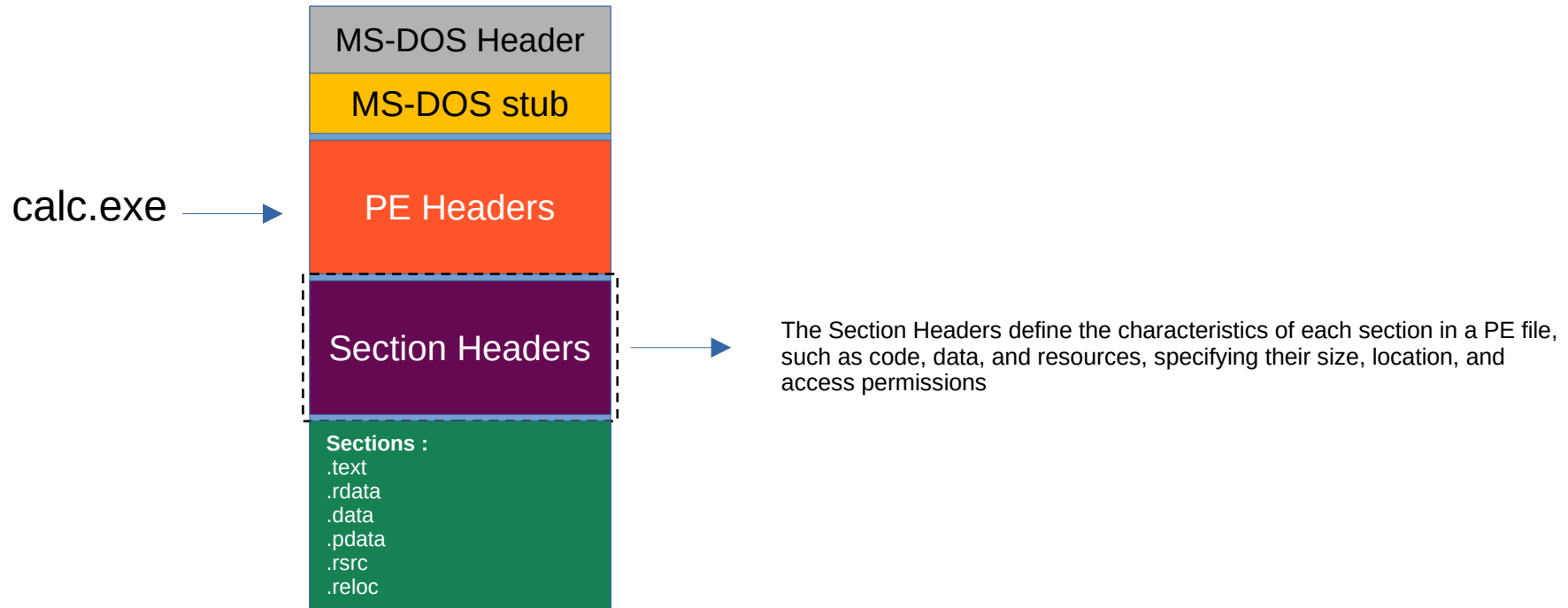
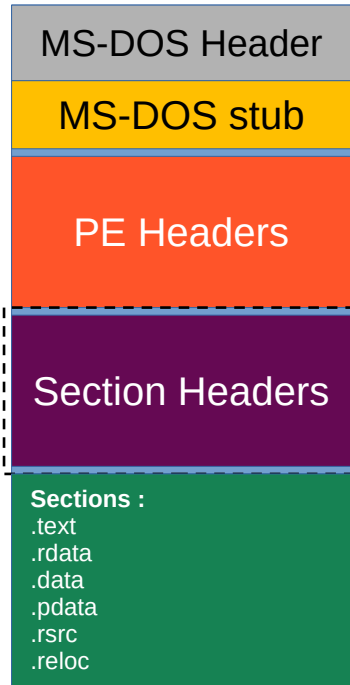


# PE file structure



# PE file structure

calc.exe



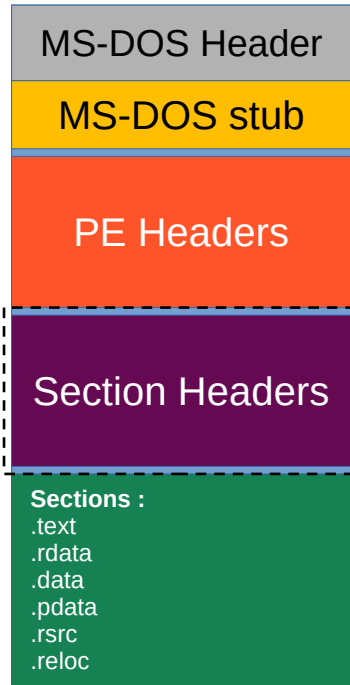
|                         |                         |
|-------------------------|-------------------------|
| 2E 74 65 78 74 00 00 00 | D0 0B 00 00 00 10 00 00 |
| 00 0C 00 00 00 04 00 00 | 00 00 00 00 00 00 00 00 |
| 00 00 00 00 20 00 00 60 | 2E 72 64 61 74 61 00 00 |
| 76 0C 00 00 00 20 00 00 | 00 0E 00 00 00 10 00 00 |
| 00 00 00 00 00 00 00 00 | 00 00 00 00 40 00 00 40 |
| 2E 64 61 74 61 00 00 00 | B8 06 00 00 00 30 00 00 |
| 00 02 00 00 00 1E 00 00 | 00 00 00 00 00 00 00 00 |
| 00 00 00 00 40 00 00 C0 | 2E 70 64 61 74 61 00 00 |
| F0 00 00 00 00 40 00 00 | 00 02 00 00 00 20 00 00 |
| 00 00 00 00 00 00 00 00 | 00 00 00 00 40 00 00 40 |
| 2E 72 73 72 63 00 00 00 | 10 47 00 00 00 50 00 00 |
| 00 48 00 00 00 22 00 00 | 00 00 00 00 00 00 00 00 |
| 00 00 00 00 40 00 00 40 | 2E 72 65 6C 6F 63 00 00 |
| 2C 00 00 00 00 A0 00 00 | 00 02 00 00 00 6A 00 00 |
| 00 00 00 00 00 00 00 00 | 00 00 00 00 40 00 00 42 |

winnt.h

```
typedef struct _IMAGE_SECTION_HEADER
{
    BYTE    Name[8];
    union
    {
        { DWORD    PhysicalAddress;
          DWORD    VirtualSize;
        } Misc;
        DWORD    VirtualAddress;
        DWORD    SizeOfRawData;
        DWORD    PointerToRawData;
        DWORD    PointerToRelocations;
        DWORD    PointerToLinenumbers;
        WORD     NumberOfRelocations;
        WORD     NumberOfLinenumbers;
        DWORD    Characteristics;
    }
} IMAGE_SECTION_HEADER
```

# PE file structure

calc.exe



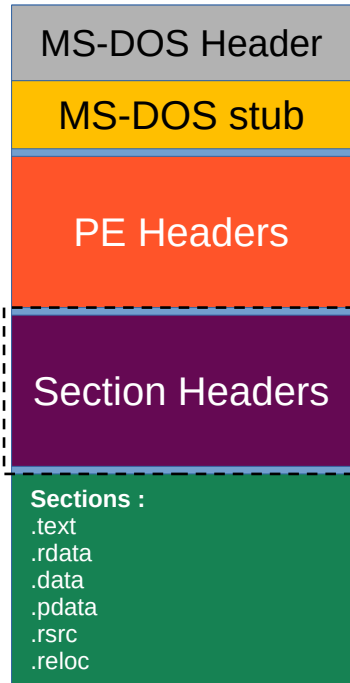
|             |             |             |
|-------------|-------------|-------------|
| .text       | D0 0B 00 00 | 00 10 00 00 |
| 00 0C 00 00 | 00 04 00 00 | 00 00 00 00 |
| 00 00 00 00 | 20 00 00 60 | .rdata      |
| 76 0C 00 00 | 00 20 00 00 | 00 0E 00 00 |
| 00 00 00 00 | 00 00 00 00 | 40 00 00 40 |
| .data       | B8 06 00 00 | 00 30 00 00 |
| 00 02 00 00 | 00 1E 00 00 | 00 00 00 00 |
| 00 00 00 00 | 40 00 00 C0 | .pdata      |
| F0 00 00 00 | 00 40 00 00 | 00 02 00 00 |
| 00 00 00 00 | 00 00 00 00 | 40 00 00 40 |
| .rsrc       | 10 47 00 00 | 00 50 00 00 |
| 00 48 00 00 | 00 22 00 00 | 00 00 00 00 |
| 00 00 00 00 | 40 00 00 40 | .reloc      |
| 2C 00 00 00 | 00 A0 00 00 | 00 02 00 00 |
| 00 00 00 00 | 00 00 00 00 | 00 6A 00 00 |
|             |             | 40 00 00 42 |

winnt.h

```
typedef struct _IMAGE_SECTION_HEADER
{
    BYTE    Name[8];
    union
    {
        DWORD    PhysicalAddress;
        DWORD    VirtualSize;
    } Misc;
    DWORD    VirtualAddress;
    DWORD    SizeOfRawData;
    DWORD    PointerToRawData;
    DWORD    PointerToRelocations;
    DWORD    PointerToLinenumbers;
    WORD     NumberOfRelocations;
    WORD     NumberOfLinenumbers;
    DWORD    Characteristics;
} IMAGE_SECTION_HEADER
```

# PE file structure

calc.exe



|             |             |             |
|-------------|-------------|-------------|
| .text       | D0 0B 00 00 | 00 10 00 00 |
| 00 0C 00 00 | 00 04 00 00 | 00 00 00 00 |
| 00 00 00 00 | 20 00 00 60 | .rdata      |
| 76 0C 00 00 | 00 20 00 00 | 00 0E 00 00 |
| 00 00 00 00 | 00 00 00 00 | 40 00 00 40 |
| .data       | B8 06 00 00 | 00 30 00 00 |
| 00 02 00 00 | 00 1E 00 00 | 00 00 00 00 |
| 00 00 00 00 | 40 00 00 C0 | .pdata      |
| F0 00 00 00 | 00 40 00 00 | 00 02 00 00 |
| 00 00 00 00 | 00 00 00 00 | 40 00 00 40 |
| .rsrc       | 10 47 00 00 | 00 50 00 00 |
| 00 48 00 00 | 00 22 00 00 | 00 00 00 00 |
| 00 00 00 00 | 40 00 00 40 | .reloc      |
| 2C 00 00 00 | 00 A0 00 00 | 00 02 00 00 |
| 00 00 00 00 | 00 00 00 00 | 00 6A 00 00 |
| 00 00 00 00 | 00 00 00 00 | 40 00 00 42 |

winnt.h

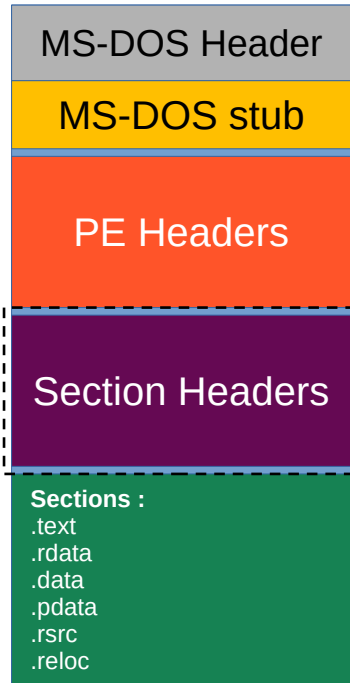
```
typedef struct _IMAGE_SECTION_HEADER
{
    BYTE    Name[8];
    union
    {
        DWORD    PhysicalAddress;
        DWORD    VirtualSize;
    } Misc;
    DWORD    VirtualAddress;
    DWORD    SizeOfRawData;
    DWORD    PointerToRawData;
    DWORD    PointerToRelocations;
    DWORD    PointerToLinenumbers;
    WORD     NumberOfRelocations;
    WORD     NumberOfLinenumbers;
    DWORD    Characteristics;
} IMAGE_SECTION_HEADER
```

## Virtual Size

This is the size of the section in memory when loaded.  
It represents the actual size needed by the section at runtime.

# PE file structure

calc.exe



|             |             |             |
|-------------|-------------|-------------|
| .text       | D0 0B 00 00 | 00 10 00 00 |
| 00 0C 00 00 | 00 04 00 00 | 00 00 00 00 |
| 00 00 00 00 | 20 00 00 60 | .rdata      |
| 76 0C 00 00 | 00 20 00 00 | 00 0E 00 00 |
| 00 00 00 00 | 00 00 00 00 | 40 00 00 40 |
| .data       | B8 06 00 00 | 00 30 00 00 |
| 00 02 00 00 | 00 1E 00 00 | 00 00 00 00 |
| 00 00 00 00 | 40 00 00 C0 | .pdata      |
| F0 00 00 00 | 00 40 00 00 | 00 02 00 00 |
| 00 00 00 00 | 00 00 00 00 | 40 00 00 40 |
| .rsrc       | 10 47 00 00 | 00 50 00 00 |
| 00 48 00 00 | 00 22 00 00 | 00 00 00 00 |
| 00 00 00 00 | 40 00 00 40 | .reloc      |
| 2C 00 00 00 | 00 A0 00 00 | 00 02 00 00 |
| 00 00 00 00 | 00 00 00 00 | 00 6A 00 00 |
| 00 00 00 00 | 00 00 00 00 | 40 00 00 42 |

winnt.h

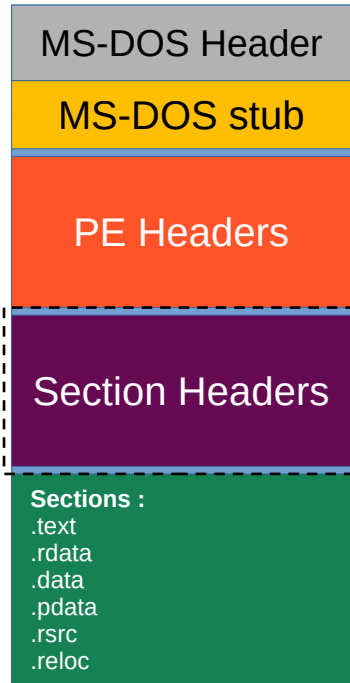
```
typedef struct _IMAGE_SECTION_HEADER
{
    BYTE    Name[8];
    union
    {
        DWORD    PhysicalAddress;
        DWORD    VirtualSize;
    } Misc;
    DWORD    VirtualAddress;
    DWORD    SizeOfRawData;
    DWORD    PointerToRawData;
    DWORD    PointerToRelocations;
    DWORD    PointerToLinenumbers;
    WORD     NumberOfRelocations;
    WORD     NumberOfLinenumbers;
    DWORD    Characteristics;
} IMAGE_SECTION_HEADER
```

## Virtual Address

This is the virtual address of the section in memory when loaded.

# PE file structure

calc.exe



|             |             |             |
|-------------|-------------|-------------|
| .text       | D0 0B 00 00 | 00 10 00 00 |
| 00 0C 00 00 | 00 04 00 00 | 00 00 00 00 |
| 00 00 00 00 | 20 00 00 60 | .rdata      |
| 76 0C 00 00 | 00 20 00 00 | 00 0E 00 00 |
| 00 00 00 00 | 00 00 00 00 | 40 00 00 40 |
| .data       | B8 06 00 00 | 00 30 00 00 |
| 00 02 00 00 | 00 1E 00 00 | 00 00 00 00 |
| 00 00 00 00 | 40 00 00 C0 | .pdata      |
| F0 00 00 00 | 00 40 00 00 | 00 02 00 00 |
| 00 00 00 00 | 00 00 00 00 | 40 00 00 40 |
| .rsrc       | 10 47 00 00 | 00 50 00 00 |
| 00 48 00 00 | 00 22 00 00 | 00 00 00 00 |
| 00 00 00 00 | 40 00 00 40 | .reloc      |
| 2C 00 00 00 | 00 A0 00 00 | 00 02 00 00 |
| 00 00 00 00 | 00 00 00 00 | 00 6A 00 00 |
|             |             | 40 00 00 42 |

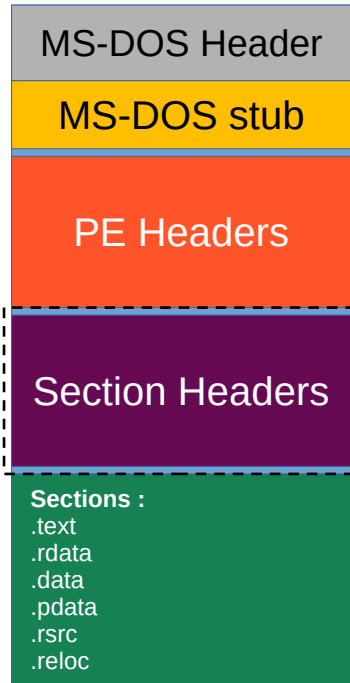
winnt.h

```
typedef struct _IMAGE_SECTION_HEADER
{
    BYTE    Name[8];
    union
    {
        DWORD    PhysicalAddress;
        DWORD    VirtualSize;
    } Misc;
    DWORD    VirtualAddress;
    DWORD    SizeOfRawData;
    DWORD    PointerToRawData;
    DWORD    PointerToRelocations;
    DWORD    PointerToLinenumbers;
    WORD     NumberOfRelocations;
    WORD     NumberOfLinenumbers;
    DWORD    Characteristics;
} IMAGE_SECTION_HEADER
```

**Size of Raw Data**  
This is the size of the section stored on disk.

# PE file structure

calc.exe



|             |             |             |
|-------------|-------------|-------------|
| .text       | D0 0B 00 00 | 00 10 00 00 |
| 00 0C 00 00 | 00 04 00 00 | 00 00 00 00 |
| 00 00 00 00 | 20 00 00 60 | .rdata      |
| 76 0C 00 00 | 00 20 00 00 | 00 0E 00 00 |
| 00 00 00 00 | 00 00 00 00 | 40 00 00 40 |
| .data       | B8 06 00 00 | 00 30 00 00 |
| 00 02 00 00 | 00 1E 00 00 | 00 00 00 00 |
| 00 00 00 00 | 40 00 00 C0 | .pdata      |
| F0 00 00 00 | 00 40 00 00 | 00 02 00 00 |
| 00 00 00 00 | 00 00 00 00 | 40 00 00 40 |
| .rsrc       | 10 47 00 00 | 00 50 00 00 |
| 00 48 00 00 | 00 22 00 00 | 00 00 00 00 |
| 00 00 00 00 | 40 00 00 40 | .reloc      |
| 2C 00 00 00 | 00 A0 00 00 | 00 02 00 00 |
| 00 00 00 00 | 00 00 00 00 | 00 6A 00 00 |
|             |             | 40 00 00 42 |

winnt.h

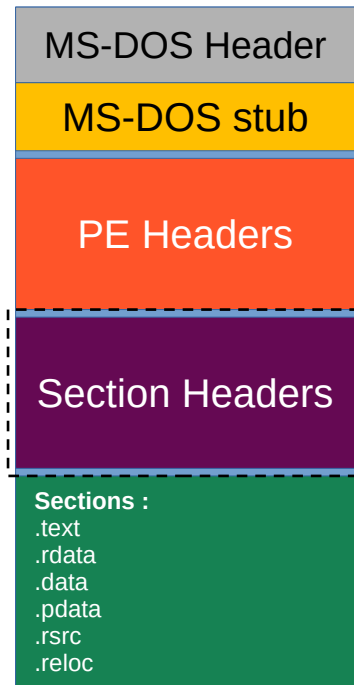
```
typedef struct _IMAGE_SECTION_HEADER
{
    BYTE    Name[8];
    union
    {
        DWORD    PhysicalAddress;
        DWORD    VirtualSize;
    } Misc;
    DWORD    VirtualAddress;
    DWORD    SizeOfRawData;
    DWORD    PointerToRawData;
    DWORD    PointerToRelocations;
    DWORD    PointerToLinenumbers;
    WORD     NumberOfRelocations;
    WORD     NumberOfLinenumbers;
    DWORD    Characteristics;
} IMAGE_SECTION_HEADER
```

### Pointer to Raw Data

This field tells you where the section's data starts in the file (on disk).

# PE file structure

calc.exe



|             |             |             |
|-------------|-------------|-------------|
| .text       | D0 0B 00 00 | 00 10 00 00 |
| 00 0C 00 00 | 00 04 00 00 | 00 00 00 00 |
| 00 00 00 00 | 20 00 00 60 | .rdata      |
| 76 0C 00 00 | 00 20 00 00 | 00 0E 00 00 |
| 00 00 00 00 | 00 00 00 00 | 40 00 00 40 |
| .data       | B8 06 00 00 | 00 30 00 00 |
| 00 02 00 00 | 00 1E 00 00 | 00 00 00 00 |
| 00 00 00 00 | 40 00 00 C0 | .pdata      |
| F0 00 00 00 | 00 40 00 00 | 00 02 00 00 |
| 00 00 00 00 | 00 00 00 00 | 40 00 00 40 |
| .rsrc       | 10 47 00 00 | 00 50 00 00 |
| 00 48 00 00 | 00 22 00 00 | 00 00 00 00 |
| 00 00 00 00 | 40 00 00 40 | .reloc      |
| 2C 00 00 00 | 00 A0 00 00 | 00 02 00 00 |
| 00 00 00 00 | 00 00 00 00 | 40 00 00 42 |

winnt.h

```
typedef struct _IMAGE_SECTION_HEADER
{
    BYTE    Name[8];
    union
    {
        DWORD    PhysicalAddress;
        DWORD    VirtualSize;
    } Misc;
    DWORD    VirtualAddress;
    DWORD    SizeOfRawData;
    DWORD    PointerToRawData;
    DWORD    PointerToRelocations;
    DWORD    PointerToLinenumbers;
    WORD     NumberOfRelocations;
    WORD     NumberOfLinenumbers;
    DWORD    Characteristics;
} IMAGE_SECTION_HEADER
```

The **Characteristics** field in the PE section header is a set of flags that describe the attributes of a section. These flags indicate whether the section contains code, data, uninitialized data, or special properties like write protection or execution permissions.

- 0x00000020 Section contains executable code.
- 0x00000040 Section contains initialized data.
- 0x00000080 Section contains uninitialized data
- 0x20000000 Section can be executed
- 0x40000000 Section can be read.
- 0x80000000 Section can be written to.
- 0x02000000 Section can be discarded after loading.
- 0x10000000 Section can be shared between processes.
- 0x04000000 Section cannot be cached in memory.