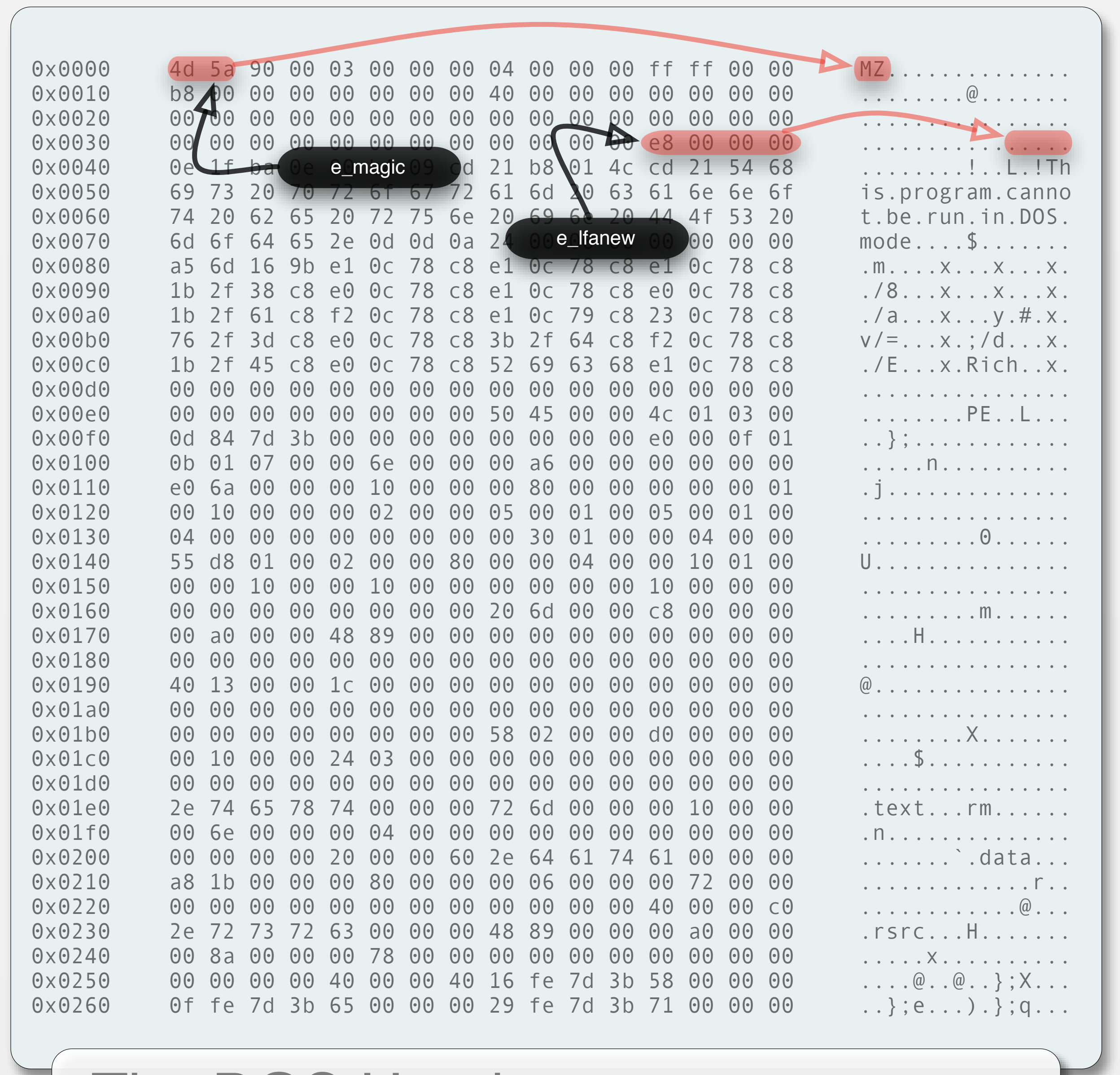
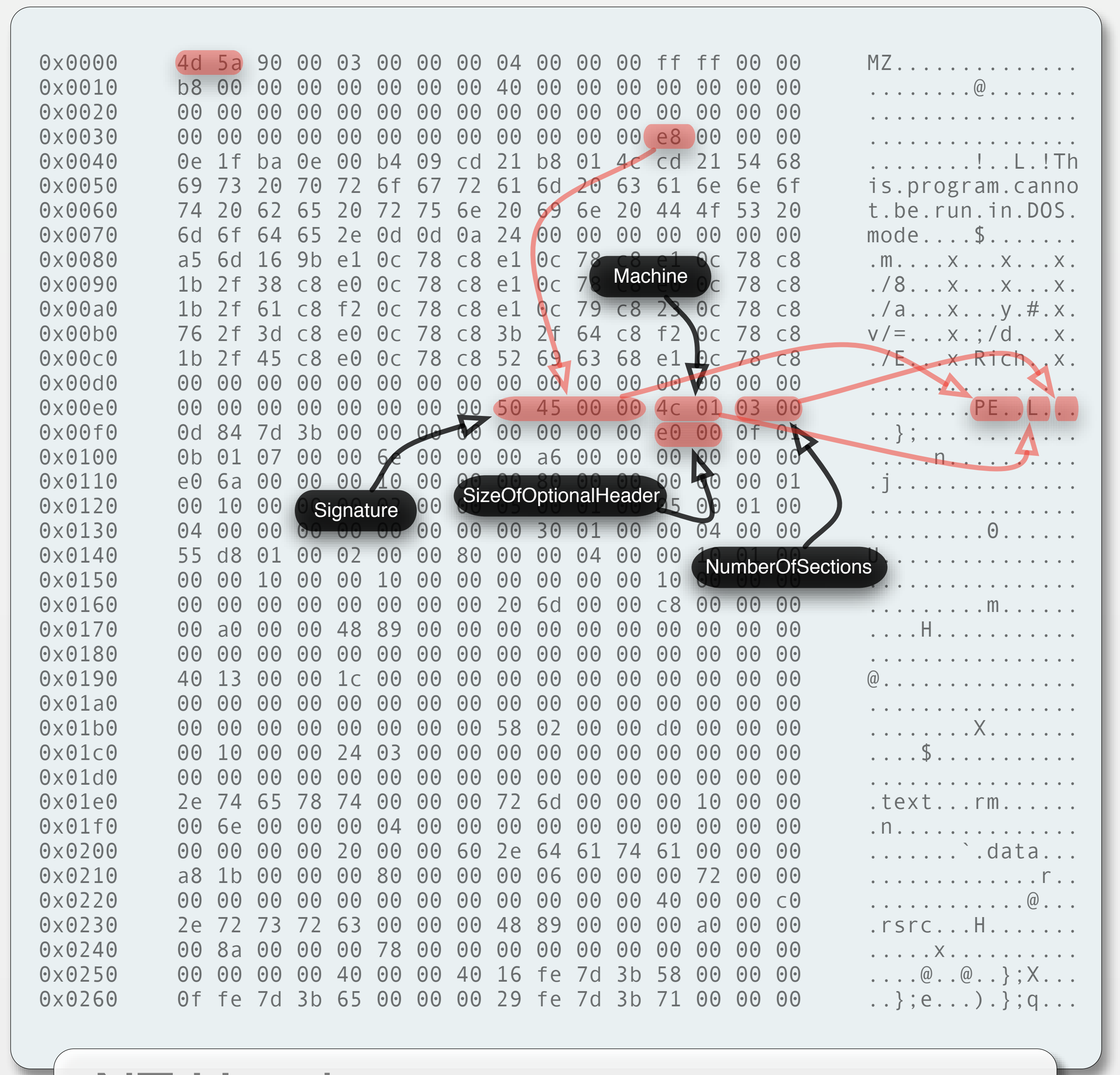
PE Header Walkthrough



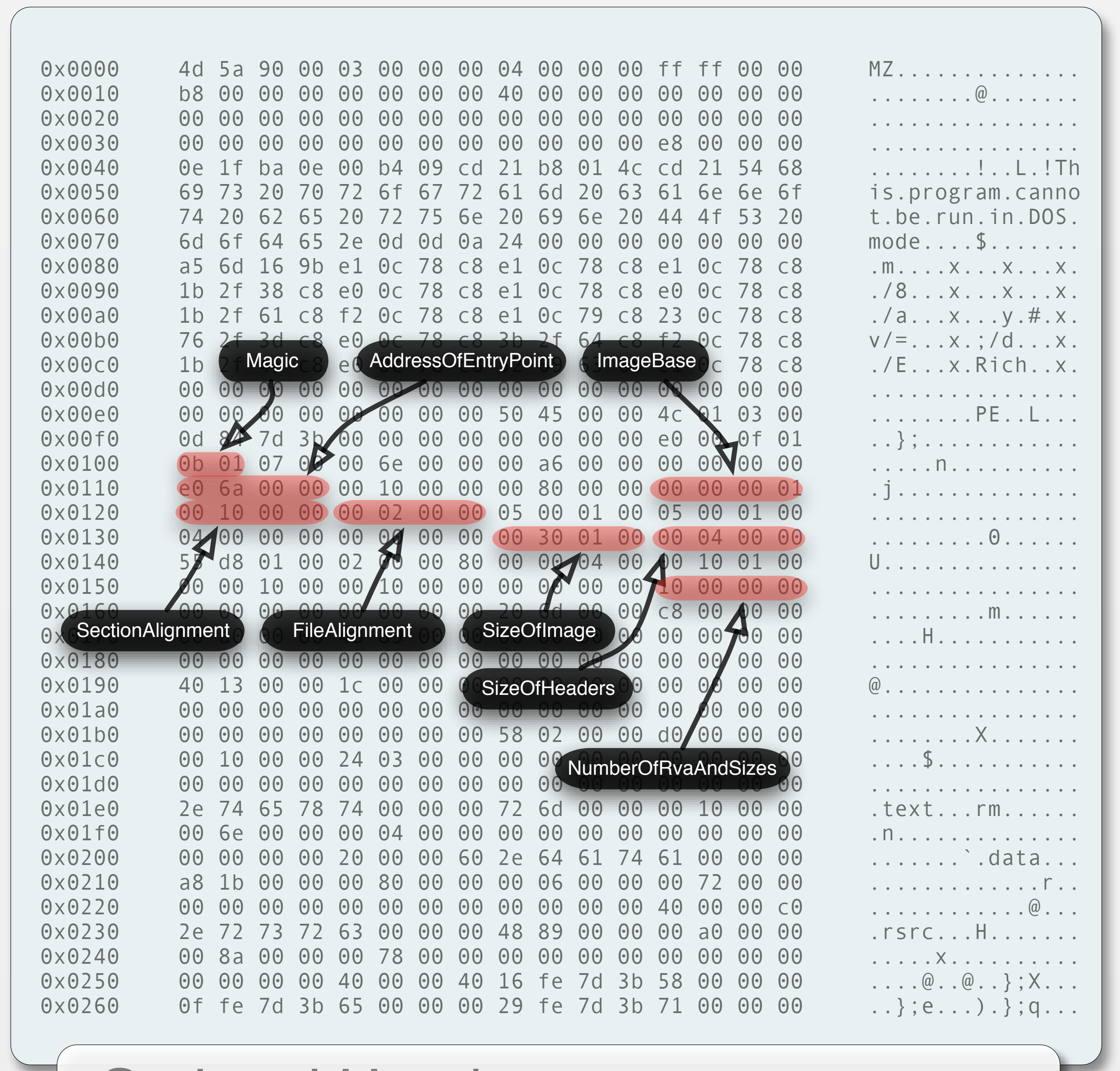
The DOS Header

The **DOS** header can be found starting at offset zero in all *Portable Executable* files. Nowadays its main objective is to indicate the offset of the main headers containing the actual information about the *PE* file, the **NT** headers. The offset where to find those headers is stored in the **e_lfanew** member.



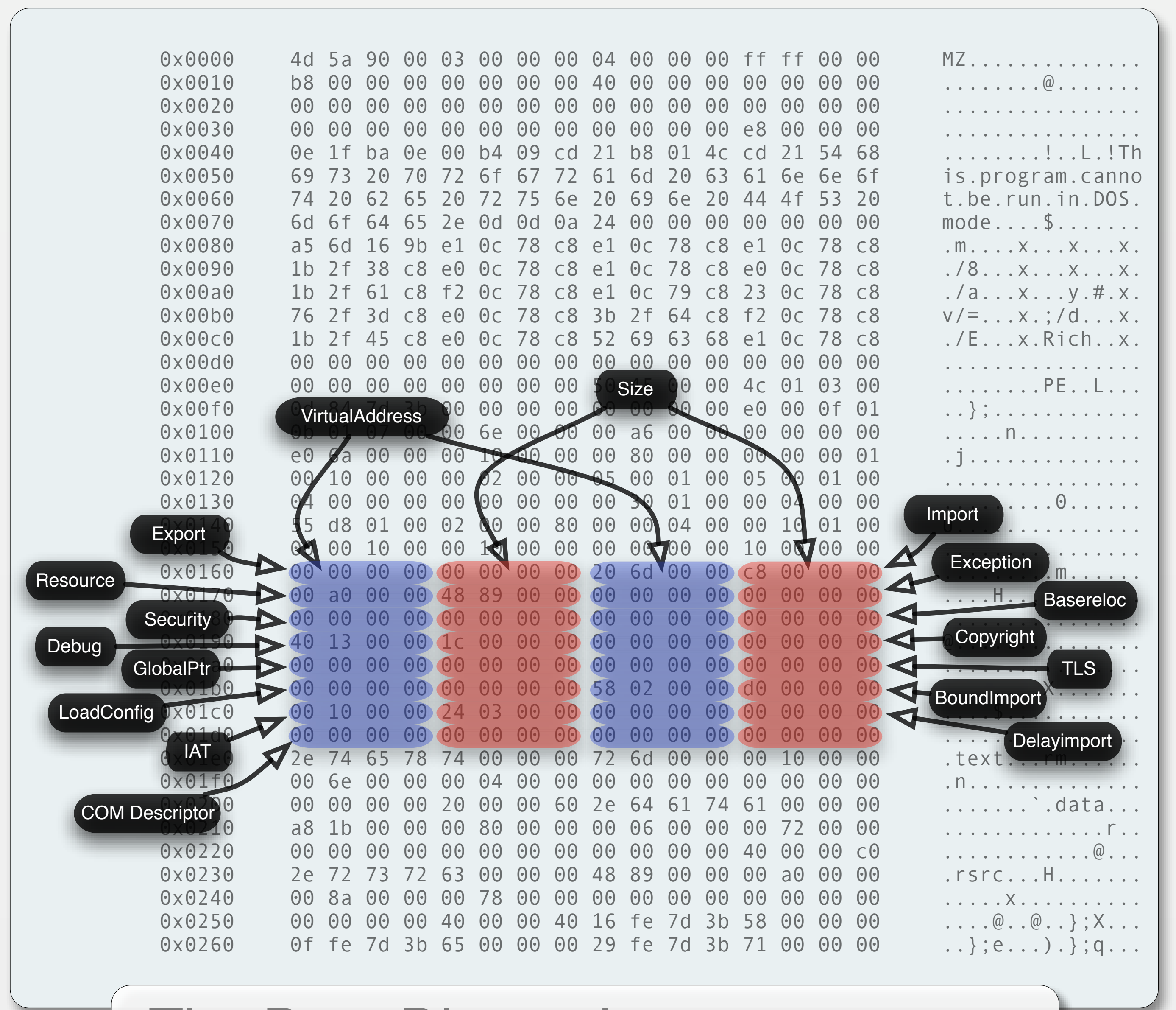
NT Headers

The **NT** headers contain three members, a signature and two other structures defining the **File** header and the **Optional** header. The signature is the standard doubleword **0x50450000** with *ASCII* representation "*PE*". Some of the important members of the **File** header are **Machine**, specifying the target architecture for which this *PE* file is compiled, and the self-describing **SizeOfOptionalHeader** and **NumberOfSections**.



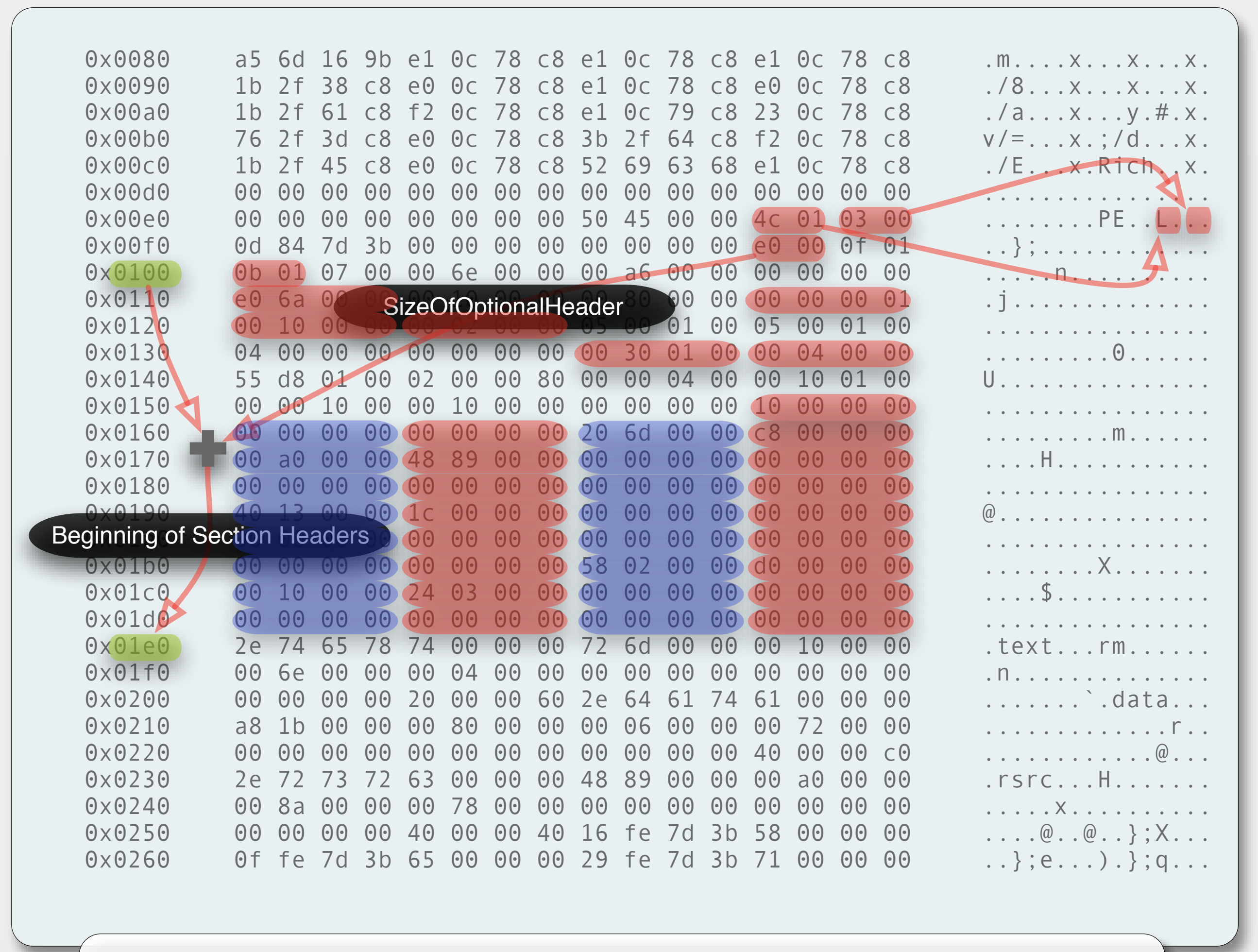
Optional Header

The **Optional** header member describes elements of the file such as the import and export directories that make possible to locate and link *DLL* libraries (which are *PE* files as well). Other entries provide structural information about the layout of the file, such as the alignment of its sections.
The slight irony behind the name *Optional* (it contains a wealth of critical information about an *EXE* or *DLL* file) comes from the fact that the *PE* format can also describe object files that are not meant to be run or otherwise need any of the information contributed by this header.



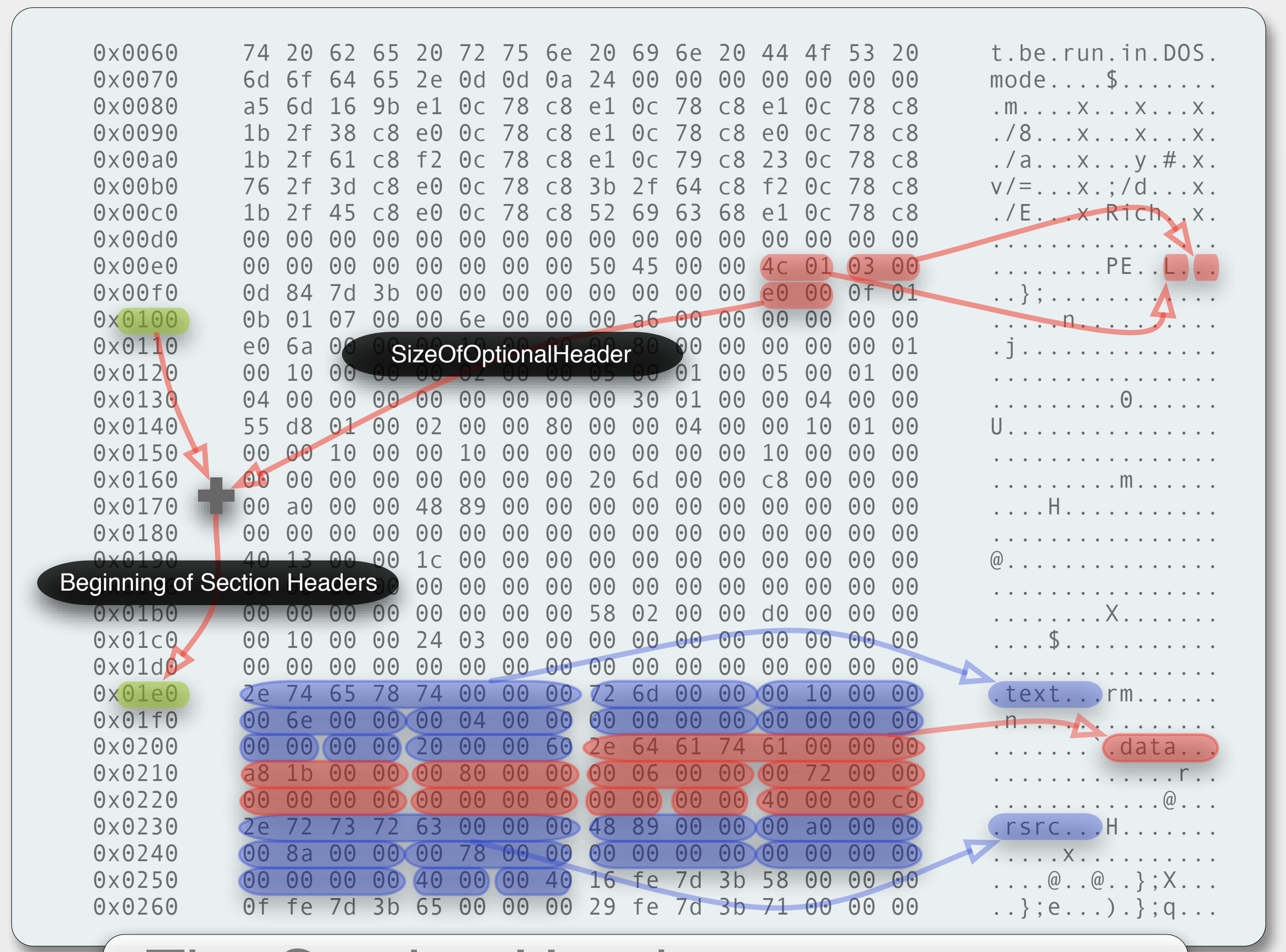
The Data Directories

These entries, contained within the **Optional** header, point to a wide selection of miscellaneous information about the file. Imported and exported symbols, debug information, resource information (icon data, version information) and others.
All of these are optional, but few *PE* files go without having a symbol import or export table that would allow them to link to (or have its symbols used by) other *PE* files.



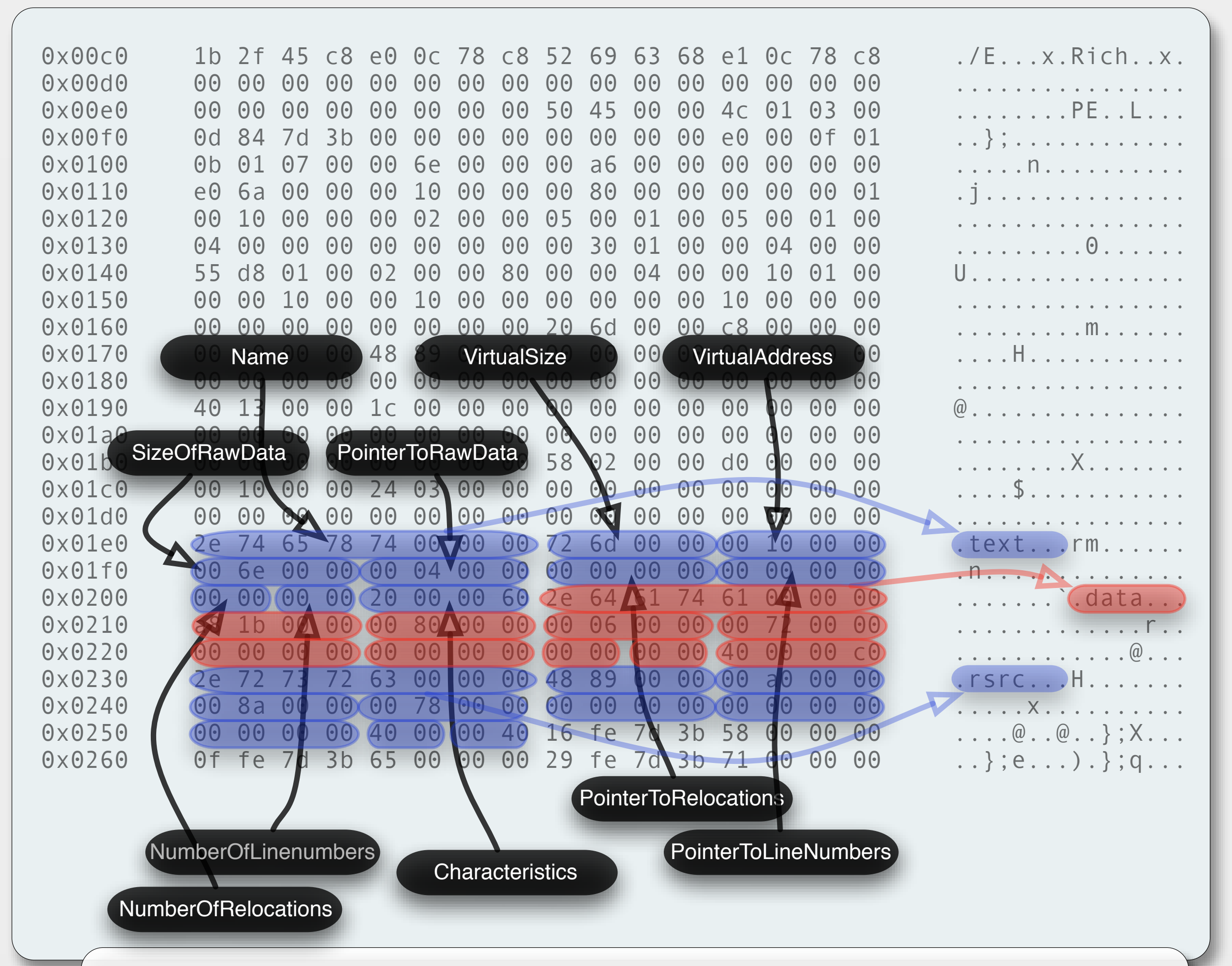
Locating the Section Headers

The **Section** headers follow immediately after the **Optional** header. The procedure to find their starting offset is to add the value from the **File** header member **SizeOfOptionalHeader** to the starting offset of the **Optional** header. The resulting value will point to the first section header. The number of sections is specified by the field **NumberOfSections** in the **File** header.



The Section Headers

The **Section** headers describe each of the sections making up the file. Sections can contain code (often referred to as text, hence the common section name '*.text*'), initialized and uninitialized data, more information describing the *PE* file itself such as resources or any other data the developer wishes to add.
There can be an arbitrary number of sections in a *PE* file.



The Section Headers

Each **Section** header structure contains the details needed to find it within the file (**PointerToRawData**), its size on disk (**SizeOfRawData**) and once loaded (**VirtualSize**) and where to load it in memory (**VirtualAddress**) relative to the **Optional** header field **ImageBase**. Whether the section contains executable code, can be read from, written to or has other properties is specified by the **Characteristics** field.

A Walk Through the PE32 Format

Display of the main headers describing the basic information contained in a *Portable Executable* file and how it maps to the data in a simple executable.

More details about the *Portable Executable* format can be found at:

http://en.wikipedia.org/wiki/Portable_Executable

OpenRCE.org