

PE Header Walkthrough

0x0000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x0010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00@.....
0x0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68!.!.!Th
0x0050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is.program.canno
0x0060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t.be.run.in.DOS.
0x0070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode...\$.
0x0080 a5 6d 16 9b e1 0c 78 c8 e1 0c 78 c8 e1 0c 78 c8 .m...x...x...x
0x0090 1b 2f 38 c8 e0 0c 78 c8 e1 0c 78 c8 e0 0c 78 c8 ./8...x...y.#.x
0x00a0 1b 2f 61 c8 f2 0c 78 c8 e1 0c 79 c8 23 0c 78 c8 ./a...x...y.#.x
0x00b0 76 2f 3d c8 e0 0c 78 c8 3b 2f 64 c8 f2 0c 78 c8 v/=...x.../d...x
0x00c0 1b 2f 45 c8 e0 0c 78 c8 52 69 63 68 e1 0c 78 c8 ./E...x.Rich..x
0x00d0 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00PE...L...
0x00e0 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00PE...L...
0x00f0 0d 84 7d 3b 00 00 00 00 00 00 00 00 e0 0f 01 ...);...n.....
0x0100 0b 01 07 00 00 00 00 00 a6 00 00 00 00 00 00 00 .j.....
0x0110 e0 6a 00 00 00 10 00 00 00 00 00 00 00 00 01
0x0120 00 10 00 00 00 02 00 00 05 00 01 05 00 01 00
0x0130 04 00 00 00 00 00 00 00 30 01 00 04 00 00
0x0140 55 d8 01 00 02 00 00 00 04 00 00 10 01 00
0x0150 00 00 10 00 00 10 00 00 00 00 00 10 00 00
0x0160 00 00 00 00 00 00 00 00 20 6d 00 00 c8 00 00
0x0170 00 a0 00 00 48 89 00 00 00 00 00 00 00 00
0x0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0190 40 13 00 00 1c 00 00 00 00 00 00 00 00 00
0x01a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x01b0 00 00 00 00 00 00 00 00 58 02 00 00 d0 00 00
0x01c0 00 10 00 00 24 03 00 00 00 00 00 00 00 00
0x01d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x01e0 2e 74 65 78 74 00 00 00 72 6d 00 00 10 00
0x01f0 00 6e 00 00 04 00 00 00 00 00 00 00 00 00
0x0200 00 00 00 20 00 00 00 00 2e 64 61 74 61 00 00
0x0210 a8 1b 00 00 00 00 00 00 05 00 00 00 72 00
0x0220 00 00 00 00 00 00 00 00 00 00 00 40 00 c0
0x0230 2e 72 73 72 63 00 00 00 48 89 00 00 a0 00
0x0240 00 8a 00 00 78 00 00 00 00 00 00 00 00 00
0x0250 00 00 00 40 00 00 40 16 fe 7d 3b 58 00 00
0x0260 0f fe 7d 3b 65 00 00 00 29 fe 7d 3b 71 00 00 ...);e...);q...

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.

0x0000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x0010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00@.....
0x0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68!.!.!Th
0x0050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is.program.canno
0x0060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t.be.run.in.DOS.
0x0070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode...\$.
0x0080 a5 6d 16 9b e1 0c 78 c8 e1 0c 78 c8 e1 0c 78 c8 .m...x...x...x
0x0090 1b 2f 38 c8 e0 0c 78 c8 e1 0c 78 c8 e0 0c 78 c8 ./8...x...y.#.x
0x00a0 1b 2f 61 c8 f2 0c 78 c8 e1 0c 79 c8 23 0c 78 c8 ./a...x...y.#.x
0x00b0 76 2f 3d c8 e0 0c 78 c8 3b 2f 64 c8 f2 0c 78 c8 v/=...x.../d...x
0x00c0 1b 2f 45 c8 e0 0c 78 c8 52 69 63 68 e1 0c 78 c8 ./E...x.Rich..x
0x00d0 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00PE...L...
0x00e0 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00PE...L...
0x00f0 0d 84 7d 3b 00 00 00 00 00 00 00 00 e0 0f 01 ...);...n.....
0x0100 0b 01 07 00 00 00 00 00 a6 00 00 00 00 00 00 00 .j.....
0x0110 e0 6a 00 00 00 10 00 00 00 00 00 00 00 00 01
0x0120 00 10 00 00 00 02 00 00 05 00 01 05 00 01 00
0x0130 04 00 00 00 00 00 00 00 30 01 00 04 00 00
0x0140 55 d8 01 00 02 00 00 00 04 00 00 10 01 00
0x0150 00 00 10 00 00 10 00 00 00 00 00 10 00 00
0x0160 00 00 00 00 00 00 00 00 20 6d 00 00 c8 00 00
0x0170 00 a0 00 00 48 89 00 00 00 00 00 00 00 00
0x0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0190 40 13 00 00 1c 00 00 00 00 00 00 00 00 00
0x01a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x01b0 00 00 00 00 00 00 00 00 58 02 00 00 d0 00 00
0x01c0 00 10 00 00 24 03 00 00 00 00 00 00 00 00
0x01d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x01e0 2e 74 65 78 74 00 00 00 72 6d 00 00 10 00
0x01f0 00 6e 00 00 04 00 00 00 00 00 00 00 00 00
0x0200 00 00 00 20 00 00 00 00 2e 64 61 74 61 00 00
0x0210 a8 1b 00 00 00 00 00 00 05 00 00 00 72 00
0x0220 00 00 00 00 00 00 00 00 00 00 00 40 00 c0
0x0230 2e 72 73 72 63 00 00 00 48 89 00 00 a0 00
0x0240 00 8a 00 00 78 00 00 00 00 00 00 00 00 00
0x0250 00 00 00 40 00 00 40 16 fe 7d 3b 58 00 00
0x0260 0f fe 7d 3b 65 00 00 00 29 fe 7d 3b 71 00 00 ...);e...);q...

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**.

0x0000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x0010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00@.....
0x0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68!.!.!Th
0x0050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is.program.canno
0x0060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t.be.run.in.DOS.
0x0070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode...\$.
0x0080 a5 6d 16 9b e1 0c 78 c8 e1 0c 78 c8 e1 0c 78 c8 .m...x...x...x
0x0090 1b 2f 38 c8 e0 0c 78 c8 e1 0c 78 c8 e0 0c 78 c8 ./8...x...y.#.x
0x00a0 1b 2f 61 c8 f2 0c 78 c8 e1 0c 79 c8 23 0c 78 c8 ./a...x...y.#.x
0x00b0 76 2f 3d c8 e0 0c 78 c8 3b 2f 64 c8 f2 0c 78 c8 v/=...x.../d...x
0x00c0 1b 2f 45 c8 e0 0c 78 c8 52 69 63 68 e1 0c 78 c8 ./E...x.Rich..x
0x00d0 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00PE...L...
0x00e0 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00PE...L...
0x00f0 0d 84 7d 3b 00 00 00 00 00 00 00 00 e0 0f 01 ...);...n.....
0x0100 0b 01 07 00 00 00 00 00 a6 00 00 00 00 00 00 00 .j.....
0x0110 e0 6a 00 00 00 10 00 00 00 00 00 00 00 00 01
0x0120 00 10 00 00 00 02 00 00 05 00 01 05 00 01 00
0x0130 04 00 00 00 00 00 00 00 30 01 00 04 00 00
0x0140 55 d8 01 00 02 00 00 00 04 00 00 10 01 00
0x0150 00 00 10 00 00 10 00 00 00 00 00 10 00 00
0x0160 00 00 00 00 00 00 00 00 20 6d 00 00 c8 00 00
0x0170 00 a0 00 00 48 89 00 00 00 00 00 00 00 00
0x0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0190 40 13 00 00 1c 00 00 00 00 00 00 00 00 00
0x01a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x01b0 00 00 00 00 00 00 00 00 58 02 00 00 d0 00 00
0x01c0 00 10 00 00 24 03 00 00 00 00 00 00 00 00
0x01d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x01e0 2e 74 65 78 74 00 00 00 72 6d 00 00 10 00
0x01f0 00 6e 00 00 04 00 00 00 00 00 00 00 00 00
0x0200 00 00 00 20 00 00 00 00 2e 64 61 74 61 00 00
0x0210 a8 1b 00 00 00 00 00 00 05 00 00 00 72 00
0x0220 00 00 00 00 00 00 00 00 00 00 00 40 00 c0
0x0230 2e 72 73 72 63 00 00 00 48 89 00 00 a0 00
0x0240 00 8a 00 00 78 00 00 00 00 00 00 00 00 00
0x0250 00 00 00 40 00 00 40 16 fe 7d 3b 58 00 00
0x0260 0f fe 7d 3b 65 00 00 00 29 fe 7d 3b 71 00 00 ...);e...);q...

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.

0x0000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x0010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00@.....
0x0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68!.!.!Th
0x0050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is.program.canno
0x0060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t.be.run.in.DOS.
0x0070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode...\$.
0x0080 a5 6d 16 9b e1 0c 78 c8 e1 0c 78 c8 e1 0c 78 c8 .m...x...x...x
0x0090 1b 2f 38 c8 e0 0c 78 c8 e1 0c 78 c8 e0 0c 78 c8 ./8...x...y.#.x
0x00a0 1b 2f 61 c8 f2 0c 78 c8 e1 0c 79 c8 23 0c 78 c8 ./a...x...y.#.x
0x00b0 76 2f 3d c8 e0 0c 78 c8 3b 2f 64 c8 f2 0c 78 c8 v/=...x.../d...x
0x00c0 1b 2f 45 c8 e0 0c 78 c8 52 69 63 68 e1 0c 78 c8 ./E...x.Rich..x
0x00d0 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00PE...L...
0x00e0 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00PE...L...
0x00f0 0d 84 7d 3b 00 00 00 00 00 00 00 00 e0 0f 01 ...);...n.....
0x0100 0b 01 07 00 00 00 00 00 a6 00 00 00 00 00 00 00 .j.....
0x0110 e0 6a 00 00 00 10 00 00 00 00 00 00 00 00 01
0x0120 00 10 00 00 00 02 00 00 05 00 01 05 00 01 00
0x0130 04 00 00 00 00 00 00 00 30 01 00 04 00 00
0x0140 55 d8 01 00 02 00 00 00 04 00 00 10 01 00
0x0150 00 00 10 00 00 10 00 00 00 00 00 10 00 00
0x0160 00 00 00 00 00 00 00 00 20 6d 00 00 c8 00 00
0x0170 00 a0 00 00 48 89 00 00 00 00 00 00 00 00
0x0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0190 40 13 00 00 1c 00 00 00 00 00 00 00 00 00
0x01a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x01b0 00 00 00 00 00 00 00 00 58 02 00 00 d0 00 00
0x01c0 00 10 00 00 24 03 00 00 00 00 00 00 00 00
0x01d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x01e0 2e 74 65 78 74 00 00 00 72 6d 00 00 10 00
0x01f0 00 6e 00 00 04 00 00 00 00 00 00 00 00 00
0x0200 00 00 00 20 00 00 00 00 2e 64 61 74 61 00 00
0x0210 a8 1b 00 00 00 00 00 00 05 00 00 00 72 00
0x0220 00 00 00 00 00 00 00 00 00 00 00 40 00 c0
0x0230 2e 72 73 72 63 00 00 00 48 89 00 00 a0 00
0x0240 00 8a 00 00 78 00 00 00 00 00 00 00 00 00
0x0250 00 00 00 40 00 00 40 16 fe 7d 3b 58 00 00
0x0260 0f fe 7d 3b 65 00 00 00 29 fe 7d 3b 71 00 00 ...);e...);q...

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.

0x0000 a5 6d 16 9b e1 0c 78 c8 e1 0c 78 c8 e1 0c 78 c8 .m...x...x...x
0x0090 1b 2f 38 c8 e0 0c 78 c8 e1 0c 78 c8 e1 0c 78 c8 ./8...x...x...x
0x00a0 1b 2f 61 c8 f2 0c 78 c8 e1 0c 79 c8 23 0c 78 c8 ./a...x...y.#.x
0x00b0 76 2f 3d c8 e0 0c 78 c8 3b 2f 64 c8 f2 0c 78 c8 v/=...x.../d...x
0x00c0 1b 2f 45 c8 e0 0c 78 c8 52 69 63 68 e1 0c 78 c8 ./E...x.Rich..x
0x00d0 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00PE...L...
0x00e0 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00PE...L...
0x00f0 0d 84 7d 3b 00 00 00 00 00 00 00 00 e0 0f 01 ...);...n.....
0x0100 0b 01 07 00 00 00 00 00 a6 00 00 00 00 00 00 00 .j.....
0x0110 e0 6a 00 00 00 10 00 00 00 00 00 00 00 00 01
0x0120 00 10 00 00 00 02 00 00 05 00 01 05 00 01 00
0x0130 04 00 00 00 00 00 00 00 30 01 00 04 00 00
0x0140 55 d8 01 00 02 00 00 00 04 00 00 10 01 00
0x0150 00 00 10 00 00 10 00 00 00 00 00 10 00 00
0x0160 00 00 00 00 00 00 00 00 20 6d 00 00 c8 00 00
0x0170 00 a0 00 00 48 89 00 00 00 00 00 00 00 00
0x0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0190 40 13 00 00 1c 00 00 00 00 00 00 00 00 00
0x01a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x01b0 00 00 00 00 00 00 00 00 58 02 00 00 d0 00 00
0x01c0 00 10 00 00 24 03 00 00 00 00 00 00 00 00
0x01d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x01e0 2e 74 65 78 74 00 00 00 72 6d 00 00 10 00
0x01f0 00 6e 00 00 04 00 00 00 00 00 00 00 00 00
0x0200 00 00 00 20 00 00 00 00 2e 64 61 74 61 00 00
0x0210 a8 1b 00 00 00 00 00 00 05 00 00 00 72 00
0x0220 00 00 00 00 00 00 00 00 00 00 00 40 00 c0
0x0230 2e 72 73 72 63 00 00 00 48 89 00 00 a0 00
0x0240 00 8a 00 00 78 00 00 00 00 00 00 00 00 00
0x0250 00 00 00 40 00 00 40 16 fe 7d 3b 58 00 00
0x0260 0f fe 7d 3b 65 00 00 00 29 fe 7d 3b 71 00 00 ...);e...);q...

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.

0x0060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t.be.run.in.DOS.
0x0070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode...\$.
0x0080 a5 6d 16 9b e1 0c 78 c8 e1 0c 78 c8 e1 0c 78 c8 .m...x...x...x
0x0090 1b 2f 38 c8 e0 0c 78 c8 e1 0c 78 c8 e0 0c 78 c8 ./8...x...y.#.x
0x00a0 1b 2f 61 c8 f2 0c 78 c8 e1 0c 79 c8 23 0c 78 c8 ./a...x...y.#.x
0x00b0 76 2f 3d c8 e0 0c 78 c8 3b 2f 64 c8 f2 0c 78 c8 v/=...x.../d...x
0x00c0 1b 2f 45 c8 e0 0c 78 c8 52 69 63 68 e1 0c 78 c8 ./E...x.Rich..x
0x00d0 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00PE...L...
0x00e0 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00PE...L...
0x00f0 0d 84 7d 3b 00 00 00 00 00 00 00 00 e0 0f 01 ...);...n.....
0x0100 0b 01 07 00 00 00 00 00 a6 00 00 00 00 00 00 00 .j.....
0x0110 e0 6a 00 00 00 10 00 00 00 00 00 00 00 00 01
0x0120 00 10 00 00 00 02 00 00 05 00 01 05 00 01 00
0x0130 04 00 00 00 00 00 00 00 30 01 00 04 00 00
0x0140 55 d8 01 00 02 00 00 00 04 00 00 10 01 00
0x0150 00 00 10 00 00 10 00 00 00 00 00 10 00 00
0x0160 00 00 00 0