peHashNG format

Hash buffer is defined as file header data and one or more section. Sections are sorted by VirtualAddress. All multi-byte values stored as unsigned integers in Big Endian format. Result of peHashNG function is SHA256 hash in hex-digest format of that buffer.

Field length in bytes	Value
2	Image Characteristics, masked for unwanted bits. mask: 0b0111111100100011
2	Subsystem.
4	SectionAlignment, rounded down to power of two
4	FileAlignment, rounded down to power of two
8	SizeOfStackCommit, rounded up to a value divisible by 4096.
8	SizeOfHeapCommit, rounded up to a value divisible by 4096.
2	Data Directory Status, masked bit flags for data directories with index from 0 to value of NumberOfRvaAndSizes -1, but not bigger than 15 : - 1 if VirtualAddress for directory is not 0 - 0 if VirtualAddress for directory is 0 - Mask: 0b0111111001111111

Table 1. peHashNG buffer for file header.

Field length in bytes	Value
4	VirtualAddress, rounded up to a value divisible by 512.
4	SizeOfRawData, rounded up to a value divisible by 512.
1	Characteristics, right shift by 24 bits, (3 least significant byte are discarded).
1	Complexity, compression ratio of section data, scaled up to 7: complexity = lenCompressedData * 7.0 / lenData - 0 if SizeOfRawData is 0 - 8 if complexity > 7 - int(round(complexity))

Table 15. peHashNG buffer for section properties.