peHash format

Hash buffer defined as file header data and one or more section data. Sections are sorted by VirtualAddress, that friendly done by “pefile” module. All multi-byte values stored as unsigned integers in Big Endian format. Result of peHash function is SHA1 hash in hex-digest format of that buffer.

Field length in bytes	Value
1	Image Characteristics, bytes are XOR-ed.
1	Subsystem, bytes are XOR-ed.
1	Stack Commit Size, rounded up to a value divisible by 4096, one least significant byte is discarded, all other bytes are XOR-ed.
1	Heap Commit Size, rounded up to a value divisible by 4096, one least significant byte is discarded, all other bytes are XOR-ed.

Table 1. peHash buffer for file header.

Field length in bytes	Value
3	VirtualAddress, right shift by 9 bits.
3	SizeOfRawData, right shift by 8 bits (one least significant byte is discarded).
1	Characteristics, right shift by 16 bits, (two least significant byte are discarded), all other bytes are XOR-ed.
1	Complexity, compression ratio of section data, scaled up to 7: complexity = int(round(lenCompressedData * 7.0 / lenData)) - 0 if SizeOfRawData is 0 - 7 if complexity > 7 - Complexity

Table 2. peHash buffer for section properties.