Windows Memory Map

2			
The upper 2 gigs are reserved for Dynamic Link Libraries (DLLs).	WINDOWS OPERATING SYSTEM DLLs and OTHER DLLs		

4294967295 — WINDOWS OPERATING SYSTEM DLLs and OTHER DLLs — $FFFFFFFF

2147483648 — $80000000

STACK — The STACK starts at the top and grows down as LOCALS are pushed onto it — 1 megabyte maximum

4 — When an EXE is double-clicked, Winodws loads his error-handling code and the rainbow pieces of the EXE.

1 — Windows gives every program its own 4-gigabyte address space.

THE HEAP — When we ask Windows for a chunk of memory for a DYNAMICALLY ALLOCATED variable, he gives it to us in this area. — 2 gigabytes minus the STACK and all the stuff below

5 — Then he loads all the DLLs listed in the IMPORT section.

6 — After that, he sets up the STACK and the HEAP.

3 — The rainbow pieces exactly match the EXE file on disk.

CODE — Compiler-generated MACHINE CODE — Varies in size

7 — Then he passes control to the first routine in the CODE section.

DATA — Compiler-generated LITERALS & GLOBALS — Varies in size

IMPORTS — List of DLLs we need — Varies in size

4198400 — $00401000

PE HEADER — Pointers to IMPORT, DATA & CODE sections — 3840 bytes

4194560 — $00400100

DOS HEADER — Leftover from DOS — 256 bytes

4194304 — $00400000

WINDOWS ERROR-HANDLING CODE — 4 megabytes

0 — $00000000