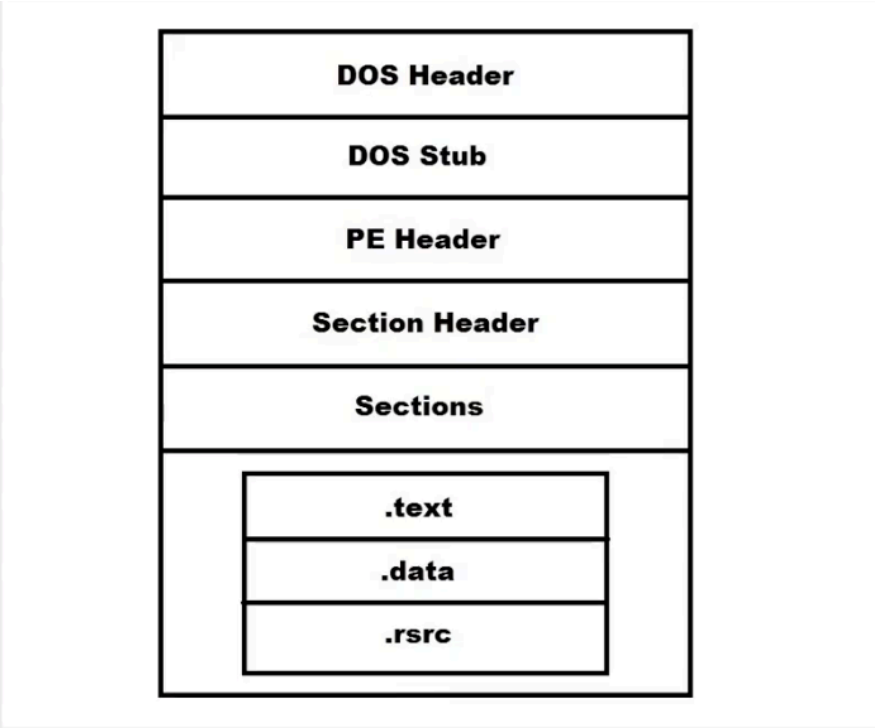
Struktur Program dan File Biner

Struktur Dasar (.EXE)



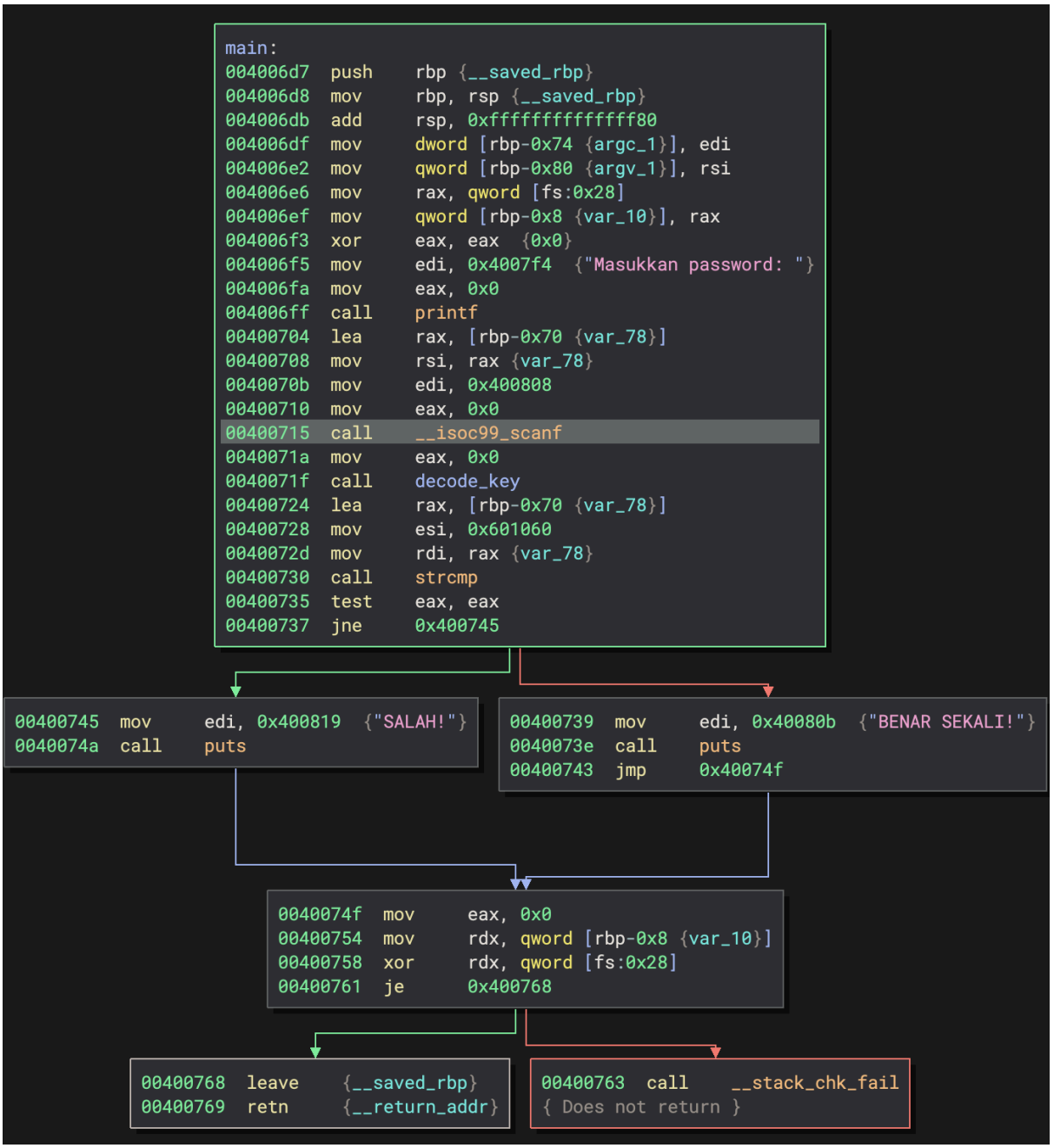
- DOS Header: bagian paling awal file, warisan dari sistem DOS lama
- DOS Stub: kode kecil yang menampilkan pesan "This program cannot be run in DOS mode"
- PE Header: informasi utama tentang file (tipe file, arsitektur, ukuran)
- Section Header: daftar yang menjelaskan isi setiap section (.text, .data, .rsrc)
- Sections: bagian isi utama file

Sections (.EXE)

Section	Deskripsi	Kegunaan
.text	Berisi instruksi program (machine code) yang dieksekusi CPU	Fokus utama dalam Reverse Engineering → Menganalisis alur logika program (disassembly, decompile).
.data	Menyimpan data yang bisa ditulis (writable data), biasanya variabel global dengan nilai awal (non-zero)	Berguna untuk melihat nilai awal variabel, tabel, atau buffer yang dimanipulasi program
.rdata	Berisi data read-only, seperti string literal dan konstanta	Sangat membantu dalam Reverse Engineering → string reference sering dipakai untuk menemukan fungsi penting
.edata	Menyimpan informasi ekspor, yaitu fungsi-fungsi yang tersedia bagi program lain (export directory)	Membantu Reverse Engineering untuk melihat API/fungsi apa saja yang diekspos ke luar
.idata	Menyimpan daftar fungsi/library yang diimpor oleh program.	Membantu melihat API eksternal apa yang dipanggil program → berguna untuk analisis malware
.pdata	Section khusus untuk informasi exception handling (structured exception handling, SEH)	Muncul di program C/C++ modern, berguna saat melacak alur error/exception

Section	Deskripsi	Kegunaan
.xdata	Menyimpan metadata tambahan untuk exception handling (berpasangan dengan .pdata)	Tidak sering dianalisis langsung, tapi penting di program besar/kompleks
.eh_frame	Dipakai oleh compiler GCC/Clang (LLVM) untuk unwinding stack saat exception	Penting kalau ingin menganalisis mekanisme error handling atau stack unwinding
.bss	Menyimpan variabel belum diinisialisasi	Bisa menunjukkan buffer besar atau array yang dipakai program
.tls	Menyimpan data yang unik untuk setiap thread dalam program	Penting kalau analisis malware multi-threading, karena data tiap thread beda
.rsrc	Berisi resources program: ikon, gambar, menu, dialog, dll.	Bisa dipakai dalam Reverse Engineering untuk menemukan UI atau pesan error yang dipakai program
.debug	Berisi informasi debug (simbol, mapping source code).	Kalau tidak dihapus, sangat berguna dalam Reverse Engineering karena memberi petunjuk nama fungsi/variabel

Graph View



Merah -> Conditional jump tidak dilakukan
Green -> Conditional jump dilakukan
Blue -> Unconditional jump
Direction up -> loop