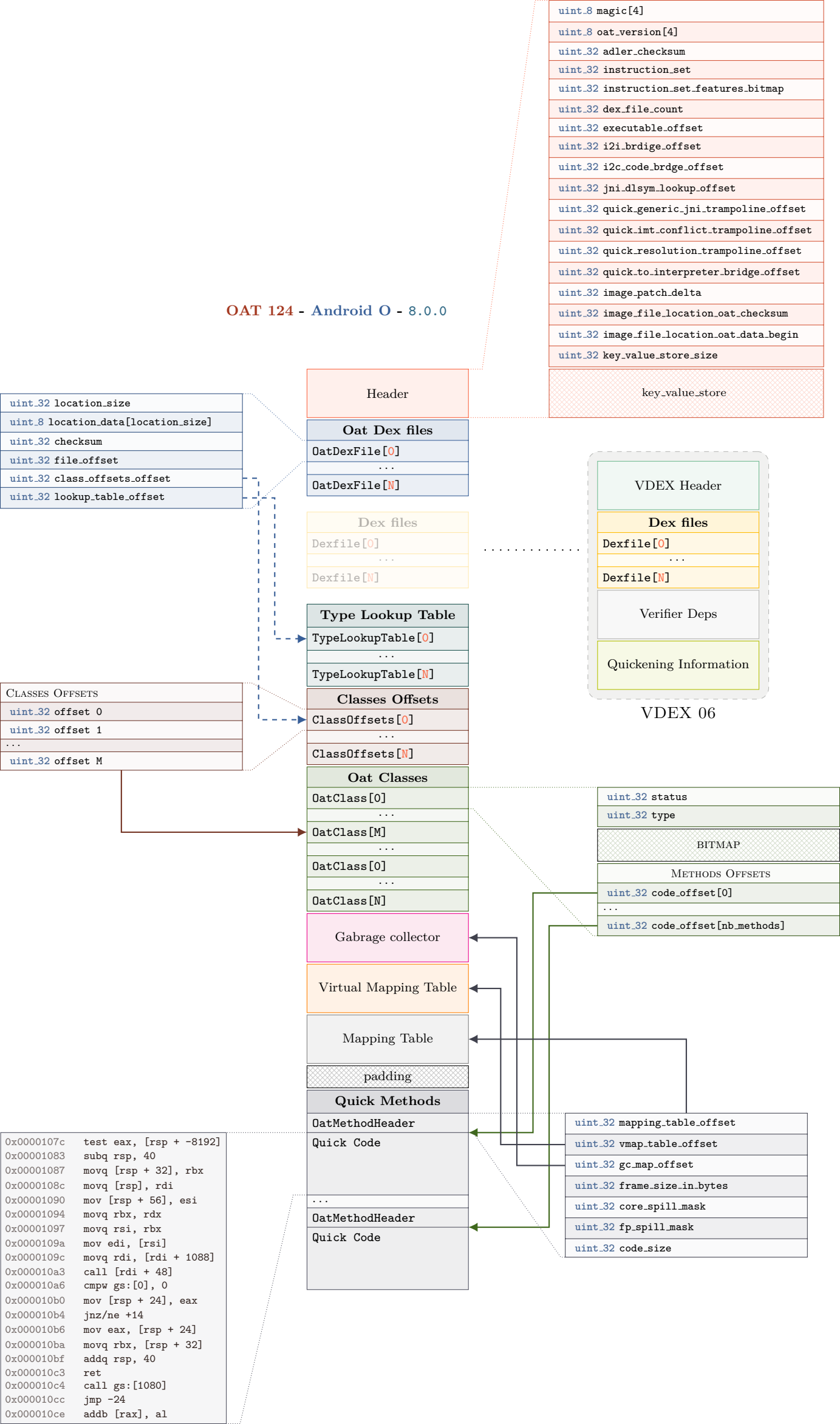
OAT 124 - Android O - 8.0.0
uint_8 magic[4]
uint_8 oat_version[4]
uint_32 adler_checksum
uint_32 instruction_set
uint_32 instruction_set_features_bitmap
uint_32 dex_file_count
uint_32 executable_offset
uint_32 i2i_brdige_offset
uint_32 i2c_code_brdge_offset
uint_32 jni_dlsym_lookup_offset
uint_32 quick_generic_jni_trampoline_offset
uint_32 quick_imt_conflict_trampoline_offset
uint_32 quick_resolution_trampoline_offset
uint_32 quick_to_interpreter_bridge_offset
uint_32 image_patch_delta
uint_32 image_file_location_oat_checksum
uint_32 image_file_location_oat_data_begin
uint_32 key_value_store_size
key_value_store
Header
Oat Dex files
OatDexFile[0]
...
OatDexFile[N]
uint_32 location_size
uint_8 location_data[location_size]
uint_32 checksum
uint_32 file_offset
uint_32 class_offsets_offset
uint_32 lookup_table_offset
Dex files
Dexfile[0]
...
Dexfile[N]
VDEX Header
Dex files
Dexfile[0]
...
Dexfile[N]
Verifier Deps
Quickening Information
VDEX 06
Type Lookup Table
TypeLookupTable[0]
...
TypeLookupTable[N]
Classes Offsets
ClassOffsets[0]
...
ClassOffsets[N]
Classes Offsets
uint_32 offset 0
uint_32 offset 1
...
uint_32 offset M
Oat Classes
OatClass[0]
...
OatClass[M]
...
OatClass[0]
...
OatClass[N]
uint_32 status
uint_32 type
BITMAP
Methods Offsets
uint_32 code_offset[0]
...
uint_32 code_offset[nb_methods]
Gabrage collector
Virtual Mapping Table
Mapping Table
padding
Quick Methods
OatMethodHeader
Quick Code
...
OatMethodHeader
Quick Code
uint_32 mapping_table_offset
uint_32 vmap_table_offset
uint_32 gc_map_offset
uint_32 frame_size_in_bytes
uint_32 core_spill_mask
uint_32 fp_spill_mask
uint_32 code_size
0x0000107c test eax, [rsp + -8192]
0x00001083 subq rsp, 40
0x00001087 movq [rsp + 32], rbx
0x0000108c movq [rsp], rdi
0x00001090 mov [rsp + 56], esi
0x00001094 movq rbx, rdx
0x00001097 movq rsi, rbx
0x0000109a mov edi, [rsi]
0x0000109c movq rdi, [rdi + 1088]
0x000010a3 call [rdi + 48]
0x000010a6 cmpw gs:[0], 0
0x000010b0 mov [rsp + 24], eax
0x000010b4 jnz/ne +14
0x000010b6 mov eax, [rsp + 24]
0x000010ba movq rbx, [rsp + 32]
0x000010bf addq rsp, 40
0x000010c3 ret
0x000010c4 call gs:[1080]
0x000010cc jmp -24
0x000010ce addb [rax], al