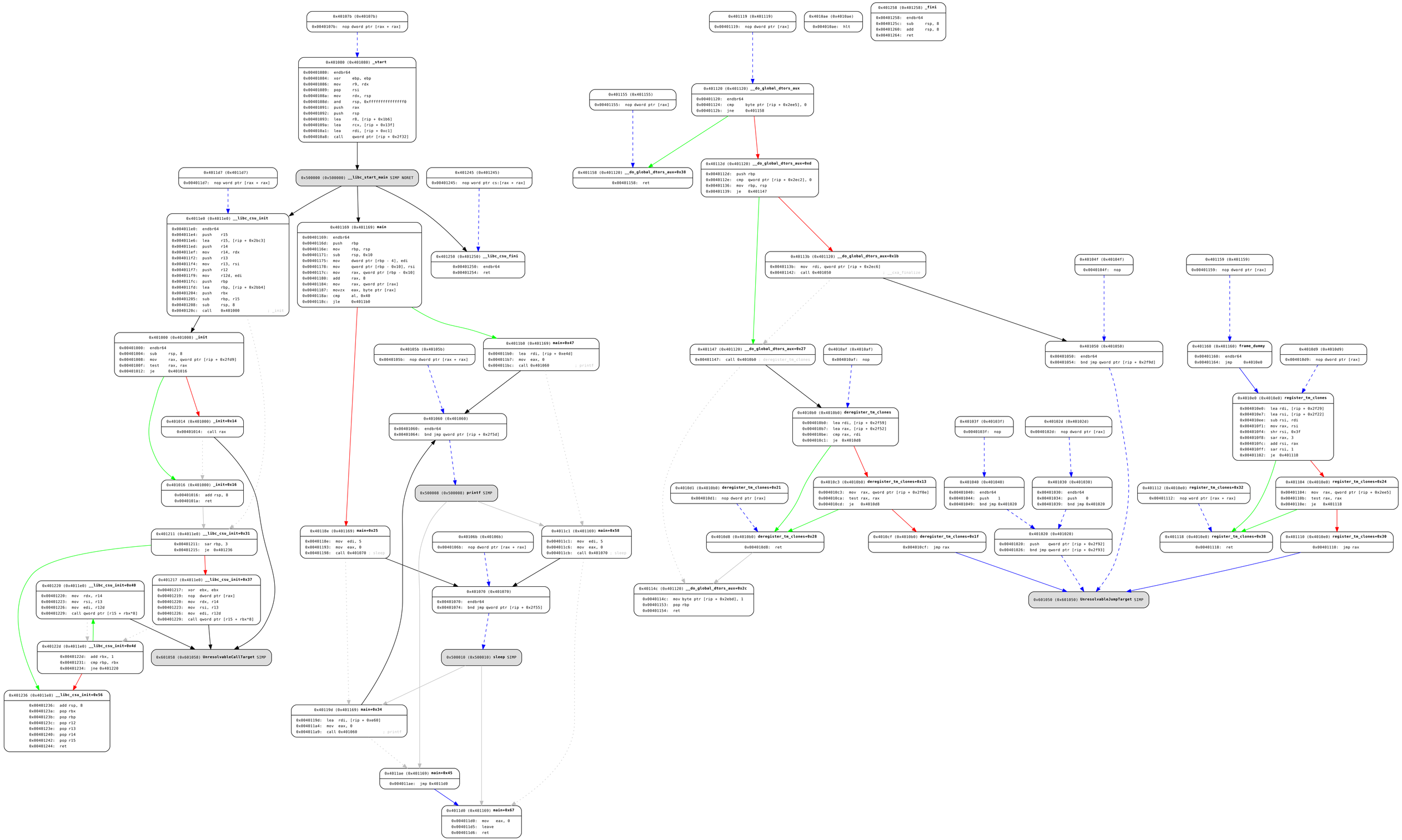
0x4010ae (0x4010ae)
0x004010ae: hlt
0x401258 (0x401258) _fini
0x0040125c: sub rsp, 8
0x00401260: add rsp, 8
0x00401264: ret
0x401119 (0x401119)
0x00401119: nop dword ptr [rax]
0x40107b (0x40107b)
0x0040107b: nop dword ptr [rax + rax]
0x401080 (0x401080) _start
0x00401080: endbr64
0x00401084: xor ebp, ebp
0x00401086: mov r9, rdx
0x00401089: pop rsi
0x0040108a: mov rdx, rsp
0x0040108d: and rsp, 0xfffffffffffffff0
0x00401091: push rax
0x00401092: push rsp
0x00401093: lea r8, [rip + 0x1b6]
0x0040109a: lea rcx, [rip + 0x13f]
0x004010a1: lea rdi, [rip + 0xc1]
0x004010a8: call qword ptr [rip + 0x2f32]
0x401155 (0x401155)
0x00401155: nop dword ptr [rax]
0x401120 (0x401120) __do_global_dtors_aux
0x00401120: endbr64
0x00401124: cmp byte ptr [rip + 0x2ee5], 0
0x0040112b: jne 0x401158
0x4011d7 (0x4011d7)
0x004011d7: nop word ptr [rax + rax]
0x500000 (0x500000) __libc_start_main SIMP NORET
0x401245 (0x401245)
0x00401245: nop word ptr cs:[rax + rax]
0x401158 (0x401120) __do_global_dtors_aux+0x38
0x00401158: ret
0x40112d (0x401120) __do_global_dtors_aux+0xd
0x0040112d: push rbp
0x0040112e: cmp qword ptr [rip + 0x2ec2], 0
0x00401136: mov rbp, rsp
0x00401139: je 0x401147
0x4011e0 (0x4011e0) __libc_csu_init
0x004011e0: endbr64
0x004011e4: push r15
0x004011e6: lea r15, [rip + 0x2bc3]
0x004011ed: push r14
0x004011ef: mov r14, rdx
0x004011f2: push r13
0x004011f4: mov r13, rsi
0x004011f7: push r12
0x004011f9: mov r12d, edi
0x004011fc: push rbp
0x004011fd: lea rbp, [rip + 0x2bb4]
0x00401204: push rbx
0x00401205: sub rbp, r15
0x00401208: sub rsp, 8
0x0040120c: call 0x401000 ; _init
0x401169 (0x401169) main
0x00401169: endbr64
0x0040116d: push rbp
0x0040116e: mov rbp, rsp
0x00401171: sub rsp, 0x10
0x00401175: mov dword ptr [rbp - 4], edi
0x00401178: mov qword ptr [rbp - 0x10], rsi
0x0040117c: mov rax, qword ptr [rbp - 0x10]
0x00401180: add rax, 8
0x00401184: mov rax, qword ptr [rax]
0x00401187: movzx eax, byte ptr [rax]
0x0040118a: cmp al, 0x40
0x0040118c: jle 0x4011b0
0x401250 (0x401250) __libc_csu_fini
0x00401250: endbr64
0x00401254: ret
0x0040113b (0x401120) __do_global_dtors_aux+0x1b
0x0040113b: mov rdi, qword ptr [rip + 0x2ec6]
0x00401142: call 0x401050 ; __cxa_finalize
0x40104f (0x40104f)
0x0040104f: nop
0x401159 (0x401159)
0x00401159: nop dword ptr [rax]
0x401000 (0x401000) _init
0x00401000: endbr64
0x00401004: sub rsp, 8
0x00401008: mov rax, qword ptr [rip + 0x2fd9]
0x0040100f: test rax, rax
0x00401012: je 0x401016
0x40105b (0x40105b)
0x0040105b: nop dword ptr [rax + rax]
0x4011b0 (0x401169) main+0x47
0x004011b0: lea rdi, [rip + 0xe4d]
0x004011b7: mov eax, 0
0x004011bc: call 0x401060 ; printf
0x401147 (0x401120) __do_global_dtors_aux+0x27
0x00401147: call 0x4010b0 ; deregister_tm_clones
0x4010af (0x4010af)
0x004010af: nop
0x401050 (0x401050)
0x00401050: endbr64
0x00401054: bnd jmp qword ptr [rip + 0x2f9d]
0x401160 (0x401160) frame_dummy
0x00401160: endbr64
0x00401164: jmp 0x4010e0
0x4010d9 (0x4010d9)
0x004010d9: nop dword ptr [rax]
0x401014 (0x401000) _init+0x14
0x00401014: call rax
0x401060 (0x401060)
0x00401060: endbr64
0x00401064: bnd jmp qword ptr [rip + 0x2f5d]
0x4010b0 (0x4010b0) deregister_tm_clones
0x004010b0: lea rdi, [rip + 0x2f59]
0x004010b7: lea rax, [rip + 0x2f52]
0x004010be: cmp rax, rdi
0x004010c1: je 0x4010d8
0x4010e0 (0x4010e0) register_tm_clones
0x004010e0: lea rdi, [rip + 0x2f29]
0x004010e7: lea rsi, [rip + 0x2f22]
0x004010ee: sub rsi, rdi
0x004010f1: mov rax, rsi
0x004010f4: shr rsi, 0x3f
0x004010f8: sar rax, 3
0x004010fc: add rsi, rax
0x004010ff: sar rsi, 1
0x00401102: je 0x401118
0x40103f (0x40103f)
0x0040103f: nop
0x40102d (0x40102d)
0x0040102d: nop dword ptr [rax]
0x401016 (0x401000) _init+0x16
0x00401016: add rsp, 8
0x0040101a: ret
0x500008 (0x500008) printf SIMP
0x4010d1 (0x4010b0) deregister_tm_clones+0x21
0x004010d1: nop dword ptr [rax]
0x4010c3 (0x4010b0) deregister_tm_clones+0x13
0x004010c3: mov rax, qword ptr [rip + 0x2f0e]
0x004010ca: test rax, rax
0x004010cd: je 0x4010d8
0x401040 (0x401040)
0x00401040: endbr64
0x00401044: push 1
0x00401049: bnd jmp 0x401020
0x401030 (0x401030)
0x00401030: endbr64
0x00401034: push 0
0x00401039: bnd jmp 0x401020
0x401112 (0x4010e0) register_tm_clones+0x32
0x00401112: nop word ptr [rax + rax]
0x401104 (0x4010e0) register_tm_clones+0x24
0x00401104: mov rax, qword ptr [rip + 0x2ee5]
0x0040110b: test rax, rax
0x0040110e: je 0x401118
0x401211 (0x4011e0) __libc_csu_init+0x31
0x00401211: sar rbp, 3
0x00401215: je 0x401236
0x40118e (0x401169) main+0x25
0x0040118e: mov edi, 5
0x00401193: mov eax, 0
0x00401198: call 0x401070 ; sleep
0x40106b (0x40106b)
0x0040106b: nop dword ptr [rax + rax]
0x4011c1 (0x401169) main+0x58
0x004011c1: mov edi, 5
0x004011c6: mov eax, 0
0x004011cb: call 0x401070 ; sleep
0x4010d8 (0x4010b0) deregister_tm_clones+0x28
0x004010d8: ret
0x4010cf (0x4010b0) deregister_tm_clones+0x1f
0x004010cf: jmp rax
0x401020 (0x401020)
0x00401020: push qword ptr [rip + 0x2f92]
0x00401026: bnd jmp qword ptr [rip + 0x2f93]
0x401118 (0x4010e0) register_tm_clones+0x38
0x00401118: ret
0x401110 (0x4010e0) register_tm_clones+0x30
0x00401110: jmp rax
0x401220 (0x4011e0) __libc_csu_init+0x40
0x00401220: mov rdx, r14
0x00401223: mov rsi, r13
0x00401226: mov edi, r12d
0x00401229: call qword ptr [r15 + rbx*8]
0x401217 (0x4011e0) __libc_csu_init+0x37
0x00401217: xor ebx, ebx
0x00401219: nop dword ptr [rax]
0x00401220: mov rdx, r14
0x00401223: mov rsi, r13
0x00401226: mov edi, r12d
0x00401229: call qword ptr [r15 + rbx*8]
0x601058 (0x601058) UnresolvableCallTarget SIMP
0x40122d (0x4011e0) __libc_csu_init+0x4d
0x0040122d: add rbx, 1
0x00401231: cmp rbp, rbx
0x00401234: jne 0x401220
0x401070 (0x401070)
0x00401070: endbr64
0x00401074: bnd jmp qword ptr [rip + 0x2f55]
0x40114c (0x401120) __do_global_dtors_aux+0x2c
0x0040114c: mov byte ptr [rip + 0x2ebd], 1
0x00401153: pop rbp
0x00401154: ret
0x601050 (0x601050) UnresolvableJumpTarget SIMP
0x500010 (0x500010) sleep SIMP
0x401236 (0x4011e0) __libc_csu_init+0x56
0x00401236: add rsp, 8
0x0040123a: pop rbx
0x0040123b: pop rbp
0x0040123c: pop r12
0x0040123e: pop r13
0x00401240: pop r14
0x00401242: pop r15
0x00401244: ret
0x40119d (0x401169) main+0x34
0x0040119d: lea rdi, [rip + 0xe60]
0x004011a4: mov eax, 0
0x004011a9: call 0x401060 ; printf
0x4011ae (0x401169) main+0x45
0x004011ae: jmp 0x4011d0
0x4011d0 (0x401169) main+0x67
0x004011d0: mov eax, 0
0x004011d5: leave
0x004011d6: ret