



MASM Mini Disassembler

A 32-bit x86 Disassembler Project in
MASM

Introduction

- The MASM Mini Disassembler is a low-level programming project aimed at creating a minimal 32-bit x86 disassembler using MASM for Windows. The tool reads raw binary code and converts it into human-readable assembly instructions, focusing on core opcodes and ModR/M decoding.

Why This Project



- STRENGTHEN UNDERSTANDING OF X86 ARCHITECTURE AND ASSEMBLY LANGUAGE.



- PRACTICE BITWISE OPERATIONS, DATA PARSING, AND CONTROL FLOW IN MASM.



- BUILD A FUNCTIONAL REVERSE-ENGINEERING TOOL.



- KEEP THE SCOPE REALISTIC AND EDUCATIONAL.

Scope and Limitations

Scope:

- Reads raw .bin files.
- Decodes basic x86 instructions.
- Prints address, hex bytes, and mnemonics.

Limitations:

- No PE parsing.
- Limited opcode set (mov, add, sub, push, pop, etc.).
- Decoding only — no execution.

Example Output

Input bytes: 55 8B EC 83 EC 10

Output:

00401000 55 push ebp

00401001 8B EC mov ebp,
esp

00401003 83 EC 10 sub esp,
0x10

Project Structure

src/ – Assembly source files
(disasm.asm, decoder.asm, etc.)

samples/ – Binary samples for
testing

tests/ – Expected outputs and
validation

build/ – Compiled executables

Implementation Plan

1. File I/O and CLI argument parser

2. Basic opcode decoding (no ModR/M)

3. ModR/M and SIB addressing

4. Control flow decoding (jmp, call)

5. Polish and robustness (hex output, bounds check)

Testing & Validation

- Compare results with ndisasm or objdump.

- Maintain golden samples in /samples and /tests.

- Fuzz testing for stability on random inputs.

Future Extensions

- Add x64 support.
- Handle instruction prefixes (0x66, 0x67, 0xF3).
- Extract and disassemble PE .text section.
- Add colored and symbolized output.

Conclusion

- The MASM Mini Disassembler is a compact yet powerful learning project, combining system-level programming, assembly knowledge, and reverse-engineering techniques. It establishes a foundation for more advanced tools and demonstrates the practicality of MASM in modern development.



Repository:

- GitHub Repository link:
<https://github.com/piotrek1459/masm-minidis>
- 