

Ian Goforth

ian.goforth@gmail.com | (901) 378-0922 | Columbus, OH | Current Secret Clearance | [Website](#) | [GitHub](#) | [LinkedIn](#)

SKILLS

- **Languages:** C, C++, Python, x86 Assembly, Bash, TypeScript
- **ML / Compilers:** PyTorch, CUDA/ROCm, MLIR, Clang/libclang, LLVM IR, Polygeist
- **Security:** AFL++, Ghidra, GDB, IDA, Binary Ninja, Angr, Wireshark, Burp Suite
- **Targets:** ELF, ARM, Embedded firmware, SDR (USRP B210), Signal processing
- **Infrastructure:** Docker, CMake, Ninja, Git, Linux
- **Certifications:** OSCP | CompTIA Security+ | Network+ | A+

PROJECTS

aletheia — AI decompiler targeting MLIR. Architecture lifts binary via Ghidra p-code to SCF+arith+memref IR, then deterministic compiler passes lower to C. Built forward (C → MLIR via Polygeist) and verification (MLIR → x86) pipelines end-to-end.

excido — Fuzzing harness generator for C/C++. Walks Clang AST to resolve every transitive dependency (types, macros, globals, functions) across translation units and emits a single self-contained file with an AFL++ harness. Tested on mbedTLS (14.9K lines, 136 cross-TU functions, 0 compilation errors).

broil-search — Multi-modal video search with pgvector. Three embedding columns (transcript, caption, image) per scene, searchable as soon as any embedding lands. Jina CLIP, Molmo 2, Voxtral Mini for captioning and transcription.

EXPERIENCE

Vulnerability Researcher

March 2023 – April 2024

Battelle

Columbus, Ohio

- Applied binary analysis, fuzzing, and protocol reverse engineering to RF/EW systems spanning 2G through 5G cellular technologies.
- Performed static and dynamic analysis of embedded modem firmware targeting proprietary DSP architectures.
- Created a 5G core and radio access network in a lab environment to apply security techniques including proxying, fuzzing, and traffic analysis with minimal supervision and direction.

Cyber Security Intern

June 2022 – August 2022

COLSA Corporation

Huntsville, Alabama

- Designed and developed encryption, authentication, authorization, and accounting (AAA) features in a Dockerized, Elastic threat-hunting product.
- Configured a multi-domain Active Directory lab with technology such as AD Certificate Services and Group Policy to simulate corporate infrastructure.
- Built specifications for \$80k order of machine learning and AI-ready server hardware to expand CyberLab for future interns.

EDUCATION

Mississippi State University

December 2022

BS in Cyber Security & Operations

Starkville, Mississippi

- Relevant Coursework: Computer Forensics, Cryptography, CyberOps, Info & Computer Security, Network Security, Data & Network Communications, Algorithms, Operating Systems