# Ruilin Wang

Edmonton, AB | 587-589-0128 | ruilin.wang517@gmail.com | linkedin.com/in/ruilin-wang001 | github.com/RWuilin
Eligible to work in Canada | Open PGWP (valid until Oct 2029)

**Cybersecurity Analyst | SOC / DFIR | Network & Software Security**

## PROFILE

Cybersecurity-focused graduate candidate with hands-on experience in DFIR, protocol security, packet analysis, Windows artefact triage, and Python security tooling. Seeking SOC Analyst, Cybersecurity Analyst, DFIR, Junior Security Engineer, or AppSec roles.

## CORE SKILLS

**DFIR & SOC:** Windows registry, LNK/USB/browser/pagefile artefacts, timeline reconstruction, evidence hashing, reporting

**Network Security:** TCP/UDP, Wireshark, TLS/HTTP/DNS, packet analysis, Bloom filters, Diffie-Hellman, Shamir Secret Sharing

**AppSec:** OWASP Top 10, secure coding review, black-box fuzzing, crash/hang triage, threat modelling

**Tools:** Python, Bash, Linux, Git, Docker, Autopsy, Volatility 3, MiTeC, Burp Suite, Nmap, SQL, JavaScript

## EDUCATION

**Master of Information Technology, Cyber Security Specialization** | University of New South Wales, Sydney, Australia | Expected Aug 2026

**Bachelor of Science in Computer Science, Minor in Mathematics** | University of Alberta, Edmonton, Canada | Dec 2024

## PROJECT EXPERIENCE

**Digital Forensics Investigation - Caelus Engineering Case** | **Autopsy, Volatility 3, Wireshark, Registry, MBOX**

- Conducted a digital forensic investigation of a simulated insider data exfiltration incident by analysing Windows disk images, memory, registry artefacts, browser evidence and network traffic.
- Reconstructed an incident timeline by correlating SAM/SOFTWARE hives, Chrome credentials/cookies, LNK files, pagefile strings, USBSTOR/SetupAPI logs, emails and packet captures.
- Identified indicators of internal data exfiltration and concealment, including post-loss file access, bulk Google Drive downloads, SanDisk USB activity, missing Prefetch files, deletions and SpyAgent traces.
- Produced recommendations for MFA, endpoint USB monitoring, DLP controls, Google Workspace log preservation, forensic imaging, hash comparison and HR/legal follow-up.

**Format-Aware Black-Box Fuzzer** | **Python, Docker, Linux** | GitHub: RWuilin/simplefuzzer

- Designed and implemented a Dockerized format-aware black-box fuzzer for stdin-driven binaries using mutation-based testing to identify crashes, hangs, slow paths, and unusual program behaviours.
- Implemented format-aware mutation strategies for CSV, JSON, XML, JPEG, and plaintext inputs, with timeout handling and reproducible crash/hang input saving.
- Added output-signature tracking as a lightweight coverage approximation to preserve inputs that triggered new behaviours.

**DIMY Contact Tracing Protocol Simulator** | **Python, TCP/UDP, Threads, Bloom Filters, Shamir Secret Sharing**

- Built a Python simulator for a privacy-preserving contact tracing protocol with frontend nodes, a backend TCP server, and a passive attacker model.
- Implemented rotating ephemeral identifiers, Shamir Secret Sharing, Bloom filter encounter storage, UDP broadcasting, and TCP request-response communication.
- Used threading, locks, and background loops to coordinate node behaviour, server upload/query operations, and interactive commands.

**OpenET 2: Remote Eye-Tracking Data Benchmarking Tools** | **Client-Based Capstone Project** | Python, Pandas, NumPy, Matplotlib, Data Validation, Visualization
UNSW | Client: Dr Peter Wagner

- Contributing to a client-based research software project extending OpenET, a Python framework for validating, visualizing, and benchmarking remote eye-tracking device data.
- Designed data quality checks for missing samples, duplicate timestamps, irregular sampling intervals, invalid gaze coordinates, incomplete recordings, and inconsistent metadata.
- Developed visualization workflows and project documentation.