Kareem Hesham

PYTHON AUTOMATION & BACKEND ENGINEER

Cairo, Egypt
karim.hesham1852@gmail.com
kareemheshaam.github.io

PROFILE

Python engineer with 5+ years of experience building production-grade automation systems, backend APIs, reverse engineering protected web applications, and developing scalable data acquisition platforms. Specializes in request-level automation, protocol analysis, and turning complex investigations into maintainable software.

EXPERIENCE

Independent Python Automation & Backend Engineer

2021 - Present | Cairo, Egypt | Remote

- Build request-level automation that reproduces protected client behavior without depending on a browser or DOM.
- Reverse engineer signatures, dynamic tokens, fingerprint challenges, obfuscated JavaScript, and Android application flows.
- Design typed FastAPI services with layered architecture, PostgreSQL, SQLAlchemy, Alembic migrations, JWT authentication, and pytest.
- Develop resilient acquisition systems with explicit session state, proxy rotation, rate-limit handling, and operational diagnostics.
- Convert investigation tooling into documented open-source utilities and publish the underlying technical research.

SELECTED OPEN SOURCE

Reqvexa

HAR-based HTTP provenance analyzer that traces cookies, tokens, headers, and request dependencies with temporal evidence; CLI and optional Flet viewer.

API Automation Platform

FastAPI service with OAuth2/JWT authentication, layered routers/services/repositories, PostgreSQL, Alembic, Docker, CI, and tests.

capture2tls

Zero-dependency converter from Charles Proxy captures to tls_client/curl_cffi code that preserves header order and protocol intent.

jsunveil

Pattern-based JavaScript deobfuscator using an isolated VM and Babel AST passes to recover strings and remove common decoys.

CORE STACK

- Python / asyncio / requests
- FastAPI / Pydantic / JWT
- SQLAlchemy / PostgreSQL
- Playwright / Selenium / Scrapy
- HTTP / HTTP/2 / TLS / CDP
- Docker / Linux / GitHub Actions
- pytest / Git / CI/CD

REVERSE ENGINEERING

- JavaScript / Node.js
- Babel / AST analysis
- Frida / JADX / Android
- Burp Suite / Charles Proxy

PUBLISHED RESEARCH

Web anti-bot stack teardown
Dynamic JavaScript, device fingerprinting, and headless challenge reproduction.

Samsung UltraHDR analysis
CWE-835 denial of service found through arm64 reversing and AFL++.

LINKS

GitHub
github.com/kareemheshaam

LinkedIn
linkedin.com/in/kareemheshaam

Writing
medium.com/@kareem.hesham