

# AAYUSH GUPTA

+918700803040   aayushguptas084@gmail.com   linkedin.com/in/hashdr1ft/   github.com/hashdr1ft

## Education

### Manav Rachna University

*Bachelor's of Technology with specialization in Cybersecurity and Threat intelligence*

Sept. 2022 – Present

Faridabad, Haryana

## Internships

### Delhi Police IFSO

*DFIR Intern*

June 2024 – August 2024

*New Delhi, Delhi*

- Leveraged advanced digital forensics tools and techniques at IFSO NCFL under expert mentorship, contributing to cybercrime investigations by analyzing data and recovering critical information, while developing a Python script to automate file recovery processes, enhancing data retrieval efficiency and bridging the gap between theoretical and practical forensics applications.

## Projects

### Password Manager | *Rust, RustCrypto, Electron*

<https://github.com/hashdr1ft/Passman>

- Built Secure Password Storage Solution: Developed a password manager in Rust with an Electron front-end, ensuring high performance and memory safety.
- Master Password Encryption: Integrated master password functionality to securely retrieve and encrypt stored passwords.
- Cross-Platform Compatibility: Designed with Electron to support seamless operation on multiple platforms, enhancing user accessibility.

### Blocksic | *Rust, Etherscan API, Blockchain Security*

<https://github.com/hashdr1ft/Blocksic>

- Developed a fast Rust CLI Tool for real-time forensic analysis of Ethereum addresses.
- Detected large transfers and transaction bursts to flag laundering, bots, and flash loans.
- Single-binary, local-first tool using Etherscan API, built for SOC and DeFi security.
- Added CLI flags, verbose mode, and timestamped reports for audit-ready outputs.

### Rustacean Chat | *Rust, Leptos, WASM, LLM*

<https://github.com/hashdr1ft/Rustacean-chat>

- Built a fully local ChatGPT-style chatbot in Rust with Leptos-based WebAssembly frontend and Tailwind styling.
- Enabled on-device inference using LLaMA-based GGML models via the `llm` crate.
- Implemented real-time streaming responses and model switching via environment config.

## Trainings | Certifications

- Let's Defend Detection Engineering** | Siem, Soar, Scripting
- Cisco Network Academy CyberOps Associate** | Malware Analysis, Cryptography, Network Intrusion Analysis SecOps, Security Monitoring
- Let's Defend Siem Engineer** | Splunk, Wazuh, Alert Tuning, Log collection and Parsing

## Skills

**Programming & Scripting:** Rust, Python, TypeScript, Bash

**Systems & Cloud:** Linux (internals, automation), AWS (GuardDuty, IAM, WAF), Docker, Kubernetes, Terraform

**Security & DFIR:** Nmap, Wireshark, Burp Suite, Suricata, Zeek, Velociraptor, YARA, Sigma, TheHive, Cortex

**Threat Detection:** SIEM/SOAR (Elastic Stack, Splunk), IOC enrichment, memory/disk forensics, log analysis

**AI & Automation:** OpenAI/Groq APIs, LangChain, RAG, Flowise, Prompt Engineering

**Frameworks & Standards:** MITRE ATT&CK, OWASP Top 10, NIST 800-53, CIS Benchmarks

**Web & Tools:** Next.js, Tailwind CSS, Git, GitHub, PostgreSQL, MongoDB

## Extracurricular

- Organized technical workshops, hackathons, and guest lectures at TechSoul as a Co-coordinator.
- Managed the official website of IEEE MRU as a webmaster, ensuring seamless access to resources and event updates.
- Published a Book chapter titled "Ethical and legal aspects of Machine learning in 5G-Enabled Smart City and Energy Grid Cyber-Defense" as the fourth author of the chapter in the book titled "Advances in AI for simulation and Optimization of Energy Systems"