AHMAD RAFI SUTANTO

Tangerang & Jakarta, Indonesia | +62 895-3831-57017 | rafisutanto@gmail.com
linkedin.com/in/rafisutanto | github.com/darflashxd | darflashxd.my.id

SUMMARY

BTL1-certified cybersecurity undergraduate at BINUS University focused on digital forensics and defensive security. Builds forensic challenges, privacy tools, and CTF infrastructure; seeking a cybersecurity internship.

EDUCATION

BINUS University, School of Computer Science | Cyber Security | 2024 - 2028 (Expected)
Jakarta, Indonesia | GPA: 3.23 / 4.00

RELEVANT EXPERIENCE & LEADERSHIP

PETIR Cyber Security, BINUS University
Member | Oct 2026 - Present | Previously Apprentice | Mar - Oct 2026
Challenge Author (Digital Forensics) | Aug 2026

- Authored forensic challenges for IFEST 2026 and BeeCTF 2026, covering LUKS encryption, ext4 carving, and a simulated malicious AUR package.
- Prepared reference writeups and validation solvers, documenting Linux CLI and FTK Imager investigation workflows.

Deputy Coordinator, R&D | Cyber Security Community, BINUS | Oct 2025 - Present

- Coordinate authors across six CTF categories and review contributions for technical accuracy and solvability.
- Built GitHub Actions workflows to sync challenge metadata with CTFd via ctfcli and deploy Docker services to a VPS over SSH.

Project Officer | National Cyber Week 2025, CSC BINUS | Oct - Dec 2025

- Coordinated competition operations, an on-site IoT hacking final, and workshops on web penetration testing and adversarial AI.

R&D Activist | Cyber Security Community, BINUS | Feb - Sep 2025

- Authored file-carving challenges for CSC CTF 2025 and mentored junior members on Volatility and Wireshark investigation workflows.

SELECTED PROJECTS

PomiCat - Privacy tooling for AI chats and documents
github.com/darflashxd/pomicat

- Built a browser extension that detects and redacts PII and derived financial values in AI chats and documents, with client-side AES-256-GCM encryption and a Cloudflare Workers relay that stores ciphertext.
- Documented an evaluation across 3 LLMs and 160 fictional chat runs; added arithmetic checks, Googlebot crawler tests, and Chrome/Firefox release builds.

darflashxd.github.io/pomicat/blog

The Poisoned AUR - BeeCTF 2026 digital forensics challenge
github.com/PETIRsec/beefest-2026-qual

- Designed an Arch Linux compromise simulation requiring correlation of package logs, shell history, systemd journal entries, ELF binaries, and extended attributes (xattr) to reconstruct the attack timeline.

PulmoAI - Chest X-ray classification
github.com/darflashxd/pulmoai

- Replaced a VGG-style CNN with MobileNetV2 using transfer learning in a Flask and React app. Academic project, not a clinical diagnostic tool.

TECHNICAL SKILLS

Forensics & IR: Volatility 3, Autopsy, FTK Imager, Eric Zimmerman Tools, Wireshark; Windows/Linux artifact analysis
Detection & SIEM: Splunk, Sysmon, Windows Event Logs (EVTX), YARA Rules, Sigma Rules
Development: Python, Bash, JavaScript/TypeScript, WebCrypto, Cloudflare Workers, Git, Docker, GitHub Actions, ctfcli
Reverse Engineering: Ghidra, x64dbg, JADX, APKTool
Frameworks: MITRE ATT&CK, NIST SP 800-61, OWASP Top 10

CERTIFICATIONS & AWARDS

Blue Team Level 1 (BTL1) | Security Blue Team | Nov 2026 | Credential ID: 710141939
3rd Place & Best CTF Solver (team) - Cyber Frontier 2026 | Nov 2026 | PETIR - nonce acak = k
Finalist - Wreck-IT 7.0, General Capture The Flag | Poltek SSN | Aug 2026 | Team HM Plenger
darflashxd.my.id/certificates/cert-wreckit-finalist.pdf