Devarjya Purkayastha

devarjya.purkayastha@gmail.com | github.com/devarjya27 | LinkedIn | devarjya27.github.io

Skills

Languages: Python, Java, C, C++, Go
Core Areas: Digital Forensics, Malware Analysis/Development, Data Structures and Algorithms, Systems Programming, Operating Systems, Computer Networks, Machine Learning, Reinforcement Learning
Management & Soft Skills: Technical Management, Problem Solving, Communication, Teamwork, Graphic Design

Technical Experience

Forensics Head **Jan. 2025 – Present**
Team Cryptonite, Manipal Institute of Technology *Manipal, Karnataka*

- Currently competing in Capture The Flag (CTF) competitions as a part of India's #2 CTF Team (as per CTFtime.org); Training Junior Members in the domain of Digital Forensics.
- Selected among 1,000+ applicants for an 18-member core technical team; contributed to a #3 national ranking on CTFtime in 2025.
- Hosted a Malware Analysis workshop for 120+ participants and mentored 20+ first years undergoing Cryptonite's recruitment process.

Research Intern **May 2026 – July 2026**
Dept. of Mathematics, Indian Institute of Technology Guwahati *Guwahati, Assam*

- Implemented and evaluated deep reinforcement learning algorithms for joint optimization of UAV trajectories, beamforming, and intelligent reflecting surface phase shifts in multi-UAV wireless networks.
- Modelled secure communication under jammer influence and compared optimization strategies through reproducible experiments and quantitative evaluation.
- Conducted research under Prof. Ashok Singh Sairam through IIT Guwahati's Summer Internship Programme 2026.

Achievements

CTF Winner: ContextCon CTF 2026 - **INR 40,000** (IIIT Hyderabad), B5 CTF 2025 - **INR 15,000** (BSides Bangalore), CyberSiege 2026 - **INR 12,000** (AIET Mangalore), TexSaw CTF 2026 (UT Dallas), Kashi CTF 2025 (IIT BHU)
CTF Podium Finishes: CRYOVAULT 2025 - **INR 27,000** (PES University) (2nd), BITSCTF 2025 (BITS Goa) (2nd), TexSAW 2025 (UT Dallas) (2nd), Codefest CTF (IIT BHU) 2025 (3rd), EHAX CTF 2025 (DTU) (3rd)

Projects

PEscan | Source Code | *Python, Volatility 3, Windows Internals*

- Developed a Volatility 3 plugin that analyzes Windows memory dumps and identifies potentially malicious Portable Executable files.
- Automated inspection of PE metadata, imports, section permissions, packing indicators, and known signatures to prioritize suspicious processes for further analysis.
- Integrated the detection workflow with Volatility's plugin architecture to produce structured, repeatable results from forensic images.

CTF Challenges | niteCTF 2025 | *C, C++, Malware Development, DFIR*

- Authored a Reverse Engineering challenge (Lament of the Seraph) focused on EDR evasion, featuring PEB walking, Win32 API hashing, Heaven's Gate transitions, and vectored exception handling.
- Authored a DFIR ransomware challenge (Ophelia's Truth) requiring memory-dump analysis, CVE exploitation traces, registry forensics, and AVI-file heuristics, along with a challenge (Google ADSense) focused on UAC bypass techniques.

Education

Manipal Institute of Technology **Aug. 2024 – Aug. 2028**
B.Tech. in Data Science and Engineering; CGPA: 8.01/10 *Manipal, Karnataka*

- Scholar Category Scholarship recipient.

Sanskriti The Gurukul **May 2012 – May 2024**
ICSE (10th Grade): 95% (Science); ISC (12th Grade): 93.25% (PCME + CS) *Guwahati, Assam*