

JAY KAWA

Mumbai, India | jaykawa56@gmail.com | +91 9867554174

“ Passionate team leader with a strong drive for continuous learning and exploring cybersecurity domains. “

EDUCATION

- **University of Mumbai** | Bachelor of Engineering - Information Technology | **2020 - 2024**
 - Secured **Distinction** (CGPA of 8.1/10) in the first six semesters.
 - Cybersecurity **Club leader**
 - Led **penetration testing** projects using Burp Suite and Metasploit frameworks

PROFESSIONAL EXPERIENCE

- **Kapuragaurai Technologies : Software Developer | Nov 2024 - Present**
 - **Project: MyFRT (my First Responder Tool)**
 - Cut manual **forensic analysis time** by **80%** by developing the tool's core automation workflows in Python.
 - Built the backend platform using **Flask** and **RESTful** APIs to handle the entire evidence lifecycle, from collection to reporting and exporting.
 - Implemented a **secure authentication system** with **JWT** tokens and **role-based access controls (RBAC)** to protect sensitive forensic data.
 - Optimized **MongoDB queries** and integrated **Elasticsearch** to ensure fast processing and keyword searching across large forensic datasets (10GB+).
 - Engineered a streamlined workflow for creating **forensic disk images** of Linux machines in standard E01 and raw (DD) formats.
 - Automated live **RAM acquisition** on Linux systems using Microsoft AVML, enabling the rapid extraction of volatile evidence for immediate analysis.

PROJECTS

- **Linux Automation Assistant (Nov 2023)**
 - Developed a Python assistant for **Linux** to simplify system administration by **executing shell commands** and automating multi-step tasks through **text** or **voice input**.
 - **Tech Stack:** Python, subprocess, SpeechRecognition, pyttsx3
- **Dynamic Data Anonymization Tool (Sep 23 - Mar 24)**
 - Completed a project with **Centre for Development of Advanced Computing (CDAC)**
 - Developed an interactive data anonymization tool with Python and Streamlit to **automatically detect** and redact **Personally Identifiable Information (PII)** from **datasets**.
 - The tool uses configurable rules to apply techniques like hashing and masking, allowing users to secure sensitive data through a simple web interface.
 - **Tech Stack:** Python, Streamlit, pandas, Faker
- **Security Operations (SIEM) Home Lab**
 - Built and configured a **virtual lab environment** to **simulate** a small enterprise network, forwarding logs from various sources to a central SIEM.
 - **Deployed** and **integrated** open-source security tools including **Wazuh** (Endpoint Security), **Snort** (Network IDS), and **Wireshark** (Packet Analysis).
 - Utilized **Splunk** for **log aggregation** and **analysis**, creating **dashboards** to visualize security events and **investigate simulated threat** scenarios.

TECHNICAL SKILLS

- **SIEM & Security Analytics:** Splunk, Elastic Stack, Wazuh, Wireshark
- **Digital Forensics (DFIR):** Autopsy, Volatility, Magnet Forensics, FTK Imager
- **Network & Vulnerability Assessment:** Snort, Nmap, OpenVAS
- **Programming & Automation:** Python, Bash Scripting, API Development
- **Operating Systems:** Linux, Windows, macOS
- **Databases:** MongoDB, MySQL, PostgreSQL
- **Offensive Security Tools:** Metasploit, Burp Suite

CERTIFICATIONS & TRAINING

- **Certifications**
 - Google Cybersecurity Professional Certificate | Jul 2024
 - TryHackme: Cyber Security 101 | Sep 2025
 - Google Technical Support Fundamentals | Apr 2021
 - Cisco Introduction to Packet Tracer | Nov 2022
 - **Hands-On Training & CTFs**
 - TryHackme, picoCTF & OverTheWire: Actively solve challenges focused on cryptography, web exploitation, and Linux command-line security.
 - **Virtual Job Simulations**
 - ANZ Australia - Cyber Security Management | Oct 2023
 - Mastercard - Cybersecurity Virtual Experience | Oct 2023
 - AIG - Shields Up: Cybersecurity Simulation | Oct 2023
-