

# Wamuyu Wachira

Nairobi, Kenya | +254701573708 | [michellewachira25@gmail.com](mailto:michellewachira25@gmail.com) |

Linkedin: [www.linkedin.com/in/wamuyu-w-293062240/](https://www.linkedin.com/in/wamuyu-w-293062240/)

---

## Profile Summary

Dedicated and detail-oriented Computer Science student with a strong foundation in digital forensics and cybersecurity principles. Passionate about analyzing and protecting digital systems, with proven problem-solving skills and a keen interest in uncovering and mitigating cyber threats. Currently honing technical expertise through academic coursework and hands-on projects, eager to contribute to a dynamic team focused on safeguarding critical data and investigating cyber incidents.

---

## Skills

Technical Skills: Mobile Forensics, Network Analysis, Digital Evidence Collection, Incident Response

Tools: Wireshark, Autopsy, Nmap, Nessus, Owasp ZAP, ILEAPP

Soft Skills: Collaboration, Decision Making, Effective Communication, Adaptability

---

## Experience

### 1. Cyber Security Trainee / CyberSafe Foundation - CyberGirls Fellowship 4.0 Cohort

MARCH 2024 - NOVEMBER 2024, REMOTE

- Gained hands-on experience in digital forensics and threat intelligence, using tools like FTK Imager, Autopsy, and Kali Linux.
- Completed certifications, including arcX Threat Intelligence (Foundational and Practitioner), ISC CC, and CompTIA Security+ content.
- Conducted a forensic analysis project on mobile applications, focusing on anti-forensic techniques and encryption, securing 1st place during the Open Day.
- Built proficiency in networking, cybersecurity concepts, and threat mitigation strategies.

### 2. Cyber Security Intern/ Enigma Big Data Labs

JUNE 2024- SEPT 2024, NAIROBI, KENYA

- Performed Vulnerability Scannings for systems using tools such as OWASP ZAP, Nessus and Metasploit
- Developed an Incident Response Plan for the Company in accordance with the NIST Framework
- Developed SDS and SRS documents for different applications during the early stages of system development
- Designed UI Workflows and User Processes for various applications being developed by the company.

---

## Education

### 1. Catholic University of Eastern Africa / BSc. Computer Science

SEPTEMBER 2022 - SEPTEMBER 2026, NAIROBI

- **Relevant Coursework:** Introduction to Networking, Cybersecurity Fundamentals, System Administration, Web Development, Object-Oriented Programming.
  - **Professional Development:** Communication Skills and Public Speaking.
- 

## Projects

### 1. Uncovering Anti-Forensic Techniques

Investigated and analyzed anti-forensic techniques used to conceal web browser activities. The project involved:

- Identifying methods used to hide or delete web browsing history, cookies, and cached data to evade forensic detection.
- Uncovering techniques such as private browsing, encryption of browser data, and manipulation of browser artifacts.
- Examining the effectiveness of forensic tools in detecting hidden or altered browser data.

### 2. Network Traffic Analysis

Developed a detailed report analyzing multiple IP addresses flagged as malicious. The report included:

- Identification of why these IPs were listed as malicious.
- Geolocation analysis to determine the physical locations of the IP addresses.
- Examination of cyberattacks associated with these IP addresses, such as phishing, malware distribution, and botnet activity

### 3. Forensic Analysis of Mobile Applications

Conducted a forensic analysis of mobile applications to recover deleted data and detect anti-forensic techniques such as encryption and obfuscation. Key tasks included:

- Analyzing Android and iOS applications (e.g., WhatsApp, Facebook) to identify and recover deleted data.
  - Utilizing tools like Autopsy, iLEAPP, and SQLite Database Browser for data extraction and analysis.
  - Detecting data manipulation patterns and uncovering attempts at data concealment.
-

