Mohamed Ashraf Abdallah

Cybersecurity Analyst | Digital Forensics & Incident Response (DFIR)

Location: Minya Al Qamh, Sharqia, Egypt
Email: mohamed.ashraf.abdallah65@gmail.com
Phone: +20 112 115 4504
LinkedIn: www.linkedin.com/in/mohamed-mooka
Portfolio: https://mohamedmooka7.github.io/

Profile

A dedicated Cybersecurity Analyst with a strong focus on Digital Forensics and Incident Response (DFIR). Passionate about uncovering digital footprints of cyber threats and transforming complex incidents into actionable intelligence.

Hands-on experience in threat detection, log analysis, and forensic investigation, enabling effective protection against sophisticated attacks. Skilled in high-pressure environments requiring quick thinking and methodical analysis.

Committed to continuous learning and leveraging cutting-edge tools to strengthen security posture. Whether analyzing malicious artifacts, hunting advanced threats, or responding to incidents, I aim to safeguard digital assets and ensure operational resilience.

Technical Skills

- **Networking & Protocols:** Deep understanding of OSI & TCP/IP models, protocol behavior, port numbers, and common vulnerabilities.
- **SOC & Threat Detection:** Wireshark (packet capture and analysis), Wazuh SIEM, Splunk (log monitoring, search, alerting), Windows event log analysis, network forensics.
- **Operating Systems:** Linux (command-line proficiency), Windows (Active Directory, domain basics).
- **Programming:** C++ (OOP fundamentals), Python scripting for automation and log parsing.
- **Cybersecurity Concepts:** Threat hunting, incident triage, vulnerability assessment, Security+ fundamentals.
- **Tools:** Wireshark, Wazuh, Splunk, VirtualBox/VMWare, fuzzing tools, Windows Event Viewer, Sysmon, Burp Suite.

Education

Zagazig University – Faculty of Computers and Information Technology
Bachelor's Degree in Computer Science | Expected Graduation: 2027

Certifications

- Network Security Practitioner (CNSP) – The SecOps Group
- Google Cybersecurity Professional Certificate
- Studied CompTIA Security+, SANS SEC450 (Blue Team Fundamentals), and eJPT content

---

Practical Experience & Projects

Ethical Hacking Trainee

National Telecommunication Institute (NTI) | *Cairo, Egypt* | *Nov 2025 – Present*

- Participating in an intensive training program focused on offensive security, penetration testing, and ethical hacking methodologies.
- Gaining hands-on experience with security tools and techniques used in real-world vulnerability assessment and exploitation scenarios.
- Enhancing understanding of network security, web application security, and defensive countermeasures.

Personal SOC Lab (Virtual Machines):

- Built and managed a custom SOC lab simulating SIEM monitoring, log analysis, and incident response workflows.
- Practiced real-time alert triage, threat detection, and containment strategies using **Wazuh and Splunk**.
- Developed Python scripts to automate log analysis and streamline SOC operations.

CyberDefenders – SOC Tier-1 & Network Forensics Labs:

- Completed practical labs in SOC operations and network forensics.
- Performed packet-level analysis, incident triage, and log correlation using Wireshark and virtual environments.

CTF Participation:

- Engaged in CTF challenges on CyberDefenders and other platforms, focusing on network analysis and digital forensics.

Vulnerability Discovery – netriders.academy:

- Conducted web security testing using fuzzing techniques and discovered a hidden sensitive file (info.php) exposing critical server information.
- Performed responsible disclosure and received a reward. Gained experience in web reconnaissance, fuzzing methodologies, and ethical reporting.

Additional Strengths

- Strong analytical and investigative mindset with practical SOC exposure.
- Calm and focused under pressure; capable of working independently or in teams.
- Excellent communication skills and technical documentation writing.
- Actively pursuing advanced blue team certifications and cybersecurity specialization.

Languages

- Arabic: Native
- English: Professional working proficiency (CEFR Level B2)