

Ahmed Mahmoud Fathy

Contact Information

- **Birthdate:** 03/09/2001
- **Nationality:** Egyptian
- **Address:** Cairo
- **Phone:** +201007103198, +201551368797
- **Email:** ahmedelsakh627@gmail.com
- **Blog:** <https://hackmd.io/@M4shl3>
- **LinkedIn:** <https://www.linkedin.com/in/m4shl3>

Education

- Faculty of Communication & Electronics, Mansoura University **[Sep 2019 – Jun 2024]**
- Grade: Very Good

Objectives

Detail-oriented and driven Cybersecurity Specialist with a focus on DFIR. I excel in analyzing Windows artifacts, practicing DFIR methodologies, and conducting in-depth mobile forensics for both Android and iOS platforms. My practical experience extends to malware analysis, data recovery, and Linux forensics, showcasing a well-rounded expertise in handling diverse forensic challenges. Committed to leveraging my technical skills and hands-on experience to contribute to advanced cybersecurity projects, I am eager to enhance and lead initiatives that push the boundaries of digital forensic analysis, incident response, and malware investigation.

Professional Experience

- **Cyber Talents Blue Team Scholarship (3 months)**
 - Completed a three-month intensive program focusing on advanced topics in cybersecurity, including SOC analysis and threat hunting. Gained hands-on experience and certification as a Cyber Talents Certified SOC Analyst and Cyber Talents Certified Threat Hunter.
- **ITI Soc Analyst Track (4 Months)**
 - Acquiring essential skills in ethical hacking, digital forensics, and incident response. Concluded with a comprehensive SOC course from EC-Council, enhancing expertise in security operations and analysis.

- **ZINAD_IT (1 Month)**
 - Acquiring essential skills in Web Pentest, Dynamic Source Code Review using Semgrep framework, Application Risk Assessment, and Theat Modeling. Concluded with tasks in each category like performing Threat Modeling through Microsoft Threat Modeling Tool.
- **Forensic Researcher (Present)**
 - Conducted in-depth forensic analysis on various digital artifacts across Windows and macOS environments.
 - Engaged in purple teaming exercises to simulate adversarial tactics and improve defensive strategies.
 - Designed and developed cybersecurity labs for the HackTheBox platform, enhancing hands-on learning experiences.

Certificates

- Android Forensics with Belkasoft
- Belkasoft Beyond the Basics: Mastering Advanced Digital Forensics Techniques
- Memory Forensics Masterclass For Incident Responders (BlackPerl)
- Certified SOC Analyst from EC-Council (CSA)
- Cyberdefence Path from Tryhackme
- Jr Penetration testing Path from Tryhackme

Achievements

- 2023: 7th place in CAT CTF
- 2023: 6th place in IEEE CTF
- 2023 :2nd place in ITI-CyberTalents CTF
- 2023: 34th place in BlackHat-MEA CTF-2023 (Qualification) / 80th (Final)
- 2023: 8th place In CyShield CTF (Final)
- 2024: 2nd place In Zinad CTF (Qualification)

Volunteering

- SOC and DFIR Circle Supervisor at CAT Reloaded (Student Activity)

Books

- The Hitchhikers Guide to DFIR
- Practical Windows Forensics
- Practical Memory Forensics

- File System Forensics Analysis by Carrier Brian
- Practical Mobile Forensics (Fourth Edition)
- Practical Linux Forensics

Languages

Arabic: Native

English: Advanced