

# Hashim Alkhateeb

407-801-9224

halkhateeb33@outlook.com

linkedin.com/in/hashim-alkhateeb

portfolio

## Education

### University of Central Florida

Master of Science in Computer Science

Orlando, FL

Bachelor of Science in Computer Science

Expected May 2026

Aug. 2021 – May 2025

- Awards: Magna Cum Laude, Bright Futures Scholar, Dean's List, President's Honor Roll
- Relevant Coursework: Malware Software Vulnerability, Cyber Operations Laboratory, Incident Response Technologies
- Clubs: Hack@UCF, KnightHacks

GPA: 3.934

## Certifications

CyberDefenders Certified CyberDefender

November 2025

CompTIA CySA+ (Cybersecurity Analyst)

June 2025

CompTIA Security+

January 2025

## Projects

### Certified CyberDefender | Elastic, Wireshark, Volatility, FTK Imager, DumpIt, Zimmerman Suite

November 2025

- Investigated full attack chains across 7+ simulated, real-world attack incidents, correlating host and network artifacts in Elastic to reconstruct initial access, lateral movement, and impact.
- Conducted over 20 hands-on labs in network, disk, and memory forensics to identify malicious activity, persistence mechanisms, and data exfiltration paths.

### SOC Homelab (Self-Hosted) | Splunk, Wazuh, Suricata, Pi-hole, Unbound, Tailscale

June 2025 – Present

- Leveraged Splunk to centralize sudo authentication logs, uncovering 14 failed login attempts in one day and building a dashboard panel to continuously track abnormal authentication patterns.
- Streamlined security monitoring by designing custom dashboards and refining rules to track file integrity and authentication events.
- Mitigated 50+ critical vulnerabilities identified by Wazuh through endpoint hardening across various systems.
- Identified and responded to simulated intrusions by correlating host-based and network-based alerts, reducing detection time by 60% through real-time Suricata log analysis.

### Android Bug Detector | Python, React, Docker, Agile, Scrum, Git

Aug. 2024 – May 2025

- Directed a 5-person Scrum team to deliver a bug-detection platform that revealed functional defects, reducing manual verification by 80%.
- Integrated secure development practices within an Agile framework, enabling the team to detect and remediate vulnerabilities earlier in the SDLC, reducing security risks and rework.

## Technical Skills

**Security Operations and Monitoring:** Threat hunting, Log analysis, SIEM, Splunk, Wazuh, OSSIM, SOAR, Nessus, OpenVAS, Burp Suite, IDS/IPS tuning, Wireshark, Nmap, Netcat, MITRE ATT&CK mapping, CVSS, OSINT, Pi-hole, Unbound, Suricata, KQL, Elastic Stack, Volatility, Yara, Zeek, Velociraptor, ZUI, FTK Imager, DumpIt, Timeline Explorer

**Digital Forensics:** Digital forensics, Memory/Disk acquisition, Network traffic analysis, Registry Explorer

**Operating Systems & Support Tools:** Windows, Linux, macOS, Command-line troubleshooting, Scripting, Automation, Powershell, Bash

**Networking & Protocols:** TCP/IP, DHCP, DNS, Firewall, ACL, Endpoint hardening

**Programming & Database:** Python, Java, JavaScript, C, Node.js, React, HTML, SQL, MongoDB, AWS, Docker, Git

**Ticketing & Collaboration:** Jira, Agile and Scrum, Slack, Google Workspace, Microsoft Suite, Github

## Experience

### Graduate Teaching Assistant - Computer Science 2

Aug 2025 – Present

University of Central Florida

Orlando, FL

- Facilitated four weekly lab sessions for 180 students, reinforcing object oriented programming and algorithms while sharpening my ability to clearly convey technical concepts to diverse audiences.
- Improved student debugging proficiency by 40% by leading 1-on-1 sessions in Java and configuring development environments.
- Coordinated with the professor and TAs to align lab content with lectures, ensuring consistent instruction.

### Teaching Assistant - Discrete Structures II

Jan. 2025 – May 2025

University of Central Florida

Orlando, FL

- Guided 70–80 students weekly through problem-solving challenges, strengthening my ability to diagnose issues and communicate technical solutions clearly.
- Monitored the Canvas discussion board and held virtual/onsite office hours, providing first-line of support.