Anjeli Pancholi

Raleigh, NC | 980.435.1177 | ✉ apancholi2002@gmail.com
GitHub | LinkedIn | Blog | Stack Overflow

Scan for Portfolio

Professional Summary

Cybersecurity & Digital Forensics student (4.0 GPA) with hands-on SOC monitoring, **incident response**, and **forensic evidence analysis.** Skilled in Python automation, Wireshark, OSForensics, FTK Imager, Autopsy, and Splunk. CCNA-trained with certifications in Python and Splunk. Seeking entry-level **SOC Analyst** or **Forensics** role to apply technical expertise in real-world investigations.

Skills

- **Forensics & IR:** OSForensics, FTK Imager, Autopsy, chain-of-custody, incident response
- **Networking & Security:** CCNA concepts, TCP/IP, routing/switching, Wireshark, SOC monitoring
- **Scripting & Automation:** Python, Bash, PowerShell, Git/GitHub
- **Systems & Virtualization:** Windows/Linux admin, VMware, cloud environments
- **Other Tools:** Splunk, Ghost Framework (Android forensics), risk assessment

Education

Wake Technical Community College – Raleigh, NC
AAS, Cybersecurity (Expected May 2026) | GPA: 4.0

- President's List (Fall & Spring 2024)
- Golden Leaf & NC Next Scholarships

Certifications

- Cisco CCNA: Introduction to Networks (Mar 2025)

- Cisco CCNA: Switching, Routing & Wireless (May 2025)
- IT Specialist: Python (May 2025)
- Splunk Fundamentals (Aug 2025)

Experience

SOC Analyst Intern (Paid) | Carolina Cyber Network – Montreat College Campus | Sept 2025 – Present

- Participating in a structured, paid training program designed to build work-ready SOC analyst skills.
- Gaining hands-on exposure to commercial and open-source security tools for scanning, scripting, and penetration testing.
- Applying cybersecurity concepts daily, including log analysis, event monitoring, and vulnerability assessment.
- Shadowing experienced analysts to understand alert triage, escalation, and incident response workflows.
- Developing practical skills for entry-level roles in SOC operations and cyber defense.

Projects

- **File System Forensics:** Recovered and analyzed digital evidence using OSForensics & FTK Imager.
- **Network Defense Labs:** Configured routers/switches, implemented ACLs, and assessed vulnerabilities (CCNA labs).
- **Python & Bash Scripting:** Automated log parsing, intrusion detection, and password hashing.
- **Network Traffic Analysis:** Captured/analyzed **10,000+ packets** in lab; identified anomalies with Wireshark.
- **Mobile Forensics:** Used Ghost Framework & ADB to extract and analyze Android device data.

Relevant Links:

- **Github:** https://anjihub.github.io/anjelipancholi.github.io/
- **Linkedin:** https://www.linkedin.com/in/anjeli-pancholi-11280b272/
- **Blog:** https://anjeli.hashnode.dev/
- **Stack Overflow:** https://stackoverflow.com/users/31226648/anjeli-p