Anjeli Pancholi

Raleigh, NC | 980.435.1177 | ✉ Anjeli Pancholi

[GitHub](#) | [LinkedIn](#) | [Stack Overflow](#)

Check out my
Portfolio here!

Professional Summary

Cybersecurity & Digital Forensics student (4.0 GPA) with hands-on SOC monitoring, incident response, and forensic analysis. Skilled in Python, Wireshark, Splunk, and forensic tools including OSForensics, FTK Imager, and Autopsy. CCNA-trained and certified, with experience in evidence recovery, mobile forensics, and network defense labs; passionate about applying skills to cybercrime investigations and digital evidence analysis.

Education

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

- President's List (Fall & Spring 2024)
- Scholarships: Golden Leaf (Fall 2024)
- Next NC (Spring 2024, Fall 2024, Summer 2025)

Certifications

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

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

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

- Participated in structured SOC analyst training with exposure to security tools, scripting, and penetration testing
- Applied log analysis, event monitoring, and vulnerability assessment; shadowed analysts on alert triage & incident response
- Developed practical skills 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, Perl, & 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
  System Workflow Visualization (Mermaid): Modeled cybersecurity workflows and data flows with diagrams

Professional Development – LinkedIn Learning

- Git Essential Training (Oct 2024) | Learning Git & GitHub (Oct 2024)
- Learning Computer Security & Internet Safety (Oct 2024) | Agile Foundations (Oct 2024)
- Fred Kofman on Managing Conflict (Oct 2024) | Change Management Foundations (Jun 2024)
- ITSM Foundations: Problem Management (Jun 2024) | DevOps Foundations (Jun 2024)
- Diversity, Equity, Inclusion, and Belonging Foundations (Jun 2024)