Chad Fry

Cybersecurity Engineer

**🏠** 208 Santa Fe Trl, Irving, TX 75063

**📞** (254) 316-1091

**✉️** Chadefry@gmail.com

**🌐** ([LinkedIn](https://www.linkedin.com/in/-chad-fry/), [GitHub](https://github.com/GlitchKraken))

# Summary

Cybersecurity Engineer with 3+ years of experience in security operations and threat analysis. I’ve a Master of Science in Cybersecurity as well asadvanced training in malware analysis and reverse engineering from Georgia Tech. Skilled in developing and deploying automated threat detection systems using Python, Snort, and network monitoring tools. Adept at log analysis, threat hunting, and incident response to mitigate sophisticated cyber threats. Dedicated to strengthening security posture through proactive monitoring and tailored defense strategies.

# Experience

## Sr Information Security Analyst- Citibank, Irving, TX

Mar 2022 - PRESENT

* Performed deep packet analysis on network traffic for more than 6 of Citi’s global accounts.
* Developed 2 different Splunk dashboards used by team to expedite manual investigations into potential DOS events, as well as potential WAF attacks.
* Engineered scripts used by team to hasten non-investigative portions of processes, saving around 30 days of time a year

## Software Engineer - CGI, Belton, TX

Oct 2019 - May 2020

* Debugged, Developed, and tested CGI “Advantage” software, using Java.
* Successfully patched longstanding logon issues for local users of Advantage-testing branch.

# Skills & tools

* [Skills]

# Projects

* **Penetration Testing** – Completed several HTB boot-to-root labs.
* **Network Monitoring** – Identified and acted on patterns for many threat actors in Wireshark- including DDOS, SQL injections, botnet/C2 activity, as well as CVA attacks and Logon Brute Forcing.
* **Advanced Malware Analysis** – Faked network responses in order to reveal malware C2 servers and discover additional behaviors. Worked with Intel PIN tool suite to automate behavior-detection/finding
* **Binary Exploitation and Reverse Engineering -** A CTF-style project where I wrote exploits/write-ups for advanced topics in Binary Exploitation: ROP chains, remote exploitation, format string vulns, heap exploits like use-after-free, double-free, heap overflows. Stack Canaries and techniques to bypass them, etc.

# Education

## Masters's degree in cyber security – Georgia Institute of Technology - Dec 2025

## Bachelor’s degree in computer science – Angelo State University – May 2019