

# Franklin Charity



St. Leonard, MD 20685 | [FranklinDCharity@gmail.com](mailto:FranklinDCharity@gmail.com) | [www.FranklinCharity.com](http://www.FranklinCharity.com)

## Summary

I am a cybersecurity professional with over 7 years of professional and academic I.T. and cybersecurity experience. I am a self-starter and quick learner who has learned and used multiple programming languages to help reduce workload stress by automating trivial tasks. I have a proven track record as a leader and mentor. I am looking to bring my unique experiences and skills to a new team to continue growing in my experience and skills and help strengthen the team's capabilities.

## Certifications

- CompTIA Security +
- EC-Council Certified Ethical Hacker
- GIAC Certified Incident Handler
- DoD Digital Media Collector
- DoD Digital Forensics Examiner

## Education

### NANO DEGREE MACHINE LEARNING | CURRENT STUDENT | UDACITY

- Intro to Machine Learning with Pytorch

### B.S INFORMATION TECHNOLOGY | DECEMBER 2019 | LIBERTY UNIVERSITY

- Major: Information Technology; Data Networking and Security
- Honors: 3.85 GPA, Sigma Beta Delta Honor Society
- Graduated Summa Cum Laude

### B.S. ENVIRONMENTAL SCIENCE | MAY 2013 | AMERICAN PUBLIC UNIVERSITY

- Major: Environmental Science

## Skills & Abilities

- |   |   |
|---|---|
| • Proficient in analytical tools                                    | • Knowledgeable in network and information security |
| • Advanced data manipulation and query skills                       | • Excellent Linux command line skills               |
| • Proficient in HTML, CSS, JavaScript, C#, SQL and Python languages | • Proven skills in DFIR tools and analysis          |
| • Excellent static malware analysis tools                           | • Proven proficiency in forensic acquisitions       |
| • Outstanding attention to detail                                   | • Superb decision-making skills                     |

## **Projects & Research**

### **HOME LAB**

I have taken multiple courses in reverse engineering, ethical hackings and malware analysis. I have used my lab as a continuing learning experience. I have built domains to learn exploitation as well as hardening using STIGs. I have explored how malware affects a system and any Indicators of Compromise that the malware or exploitation attempt leave behind. Any time I have a question about how a tool is used in a forensics investigation, or how to exploit and identify a new vulnerability I have stood up an environment in my home lab. The skills learned through these activities have improved my efficiency and abilities in the workplace.

### **INFORMATION SECURITY BLOG**

I write a blog about information security topics such as malware threats, CTF walkthroughs, and new tactics and tools. I use this as an opportunity to learn more about the threat landscape and encourage myself to investigate and research emerging threats and Advanced Persistent Threats. In some of my blog posts I use it as an opportunity to teach non-technical people about different malware threats.

## **Experience**

### **DEFENSIVE CYBER OPERATIONS ANALYST | NAWCAD | 08/17/2020 – PRESENT**

- Led projects related to enhancing the capabilities of the Cyber Warfare Department in Digital forensics and Incident response, as well as, building threat hunting capabilities.
- Responded to incidents on NAVAIR owned information technology systems.
- Performed forensically sound collections of volatile and non-volatile memory to perform analysis.
- Worked independently on Cyber Warfare Detachment projects to automate already existing capabilities.
- Took ownership and updated the training plan for the Defensive Cyber Operations Branch.
- Created procedures for incident response and threat hunting.

### **IT DIRECTOR | LTCPCMS | 06/13/2016 – 08/17/2020**

- Improved efficiency by automating processes using SSMS, SSIS, Python scripting, and PowerShell.
- Led daily I.T. activities and managed outsourced I.T assets to ensure accurate completion of projects.
- Transitioned the organization to a password management platform and strengthened password policies to prevent password reuse and to secure passwords.
- Created and implemented an acceptable use policy, password policy, and clean desk policy.
- Managed and monitored user accounts within the company
- Led company security awareness trainings.
- Utilized auditing software to create alerts and daily reports highlighting non-compliance with company policies.

### **CLINICAL HUB MANAGER | LTCPCMS | 07/2014 – 06/2016**

- Led a team of 16 to 2 million dollars of savings for clients.
- Analyzed financial documents to uncover trends in pharmacy costs.
- Managed finances by reviewing invoices and consulting with long-term care facilities.
- Learned analysis techniques and social engineering pretexting and mirroring to effectively lead a team.

### **LEAD PHARMACY TECHNICIAN CPHT | RXCONNEX PHARMACY | 09/2013 – 07/2014**

- Lead the Pharmacy in Daily activities.
- Worked with IT staff to find efficiencies in daily tasks by automating cumbersome tasks.
- Learned how to properly handle and dispose of confidential patient information.

## **Additional Experience**

### **VOLUNTEERING EXPERIENCE**

- Richmond Running Meetup Group Leader
- Chapel RVA Small Group leader/ Missional Group Leadership
- Life Church Calvert Production Team

### **CAPTURE THE FLAGS AND ADDITIONAL COURSES**

- First Place Finish in the Cover6 Solutions BlueTeam CTF
- Top 10 finish in the BSidesNOVA CTF
- BSidesDC 2018 Capture the flag for noobz.
- BSidesDC 2019 Forensics workshop and competition.
- PicoCTF 2018 and 2019 Participant.
- Completed Over the Wire Bandit wargame.
- DC3 Introduction to Networks Computers and Hardware
- DC3 Log Analysis Course
- DC3 Cyber Incident Response Course
- DC3 Windows Forensics Examiner-Encase course
- Blackhat USA 2022 A complete Practical Approach to Malware Analysis & Memory Forensics course

### **OTHER ACCOMPLISHMENTS**

- Completed Cybrary SOC Analyst 1 Career Path
- Took part in the Active Countermeasures/Black Hills Infosec Threat Hunter six-hour course.
- Brad Duncan's Malware Analysis Using Wireshark class at BSidesNOVA
- Completed the SANS SEC504 Course and passed the Certification with a 92%.
- Member of the SANS Advisory Board