**Chad Walker**

Chad.walker34@outlook.com

**Python Developer**

Python Developer with more than five years of experience in Development, Automation, Maintaining and Testing Software Quality for client/server and web based products. Proficient in full Software Development Life Cycle (Waterfall and Agile), including requirement analysis, test planning, effort estimation, execution, defect management, delivery, and support. ***Areas of technical expertise include:***

**Programming languages**: Python, C / C++, Java and SQL

**Web Technologies**: Django, HTML, HTML5, CSS, Bootstrap, PHP, Java Script, REST Requests/Responses

**Database Tools**: PostgreSQL, Sqlite, MySQL, Microsoft SQL Server Management Studio

**Scripting**: Bash Shell, VBScript, JavaScript and Groovy Script.

**Network Tools**: Wireshark, tshark, Tcpdump, Nmap, Airodump-ng, hping3, Kali frameworks.

**Protocols**: OSI Model, TCP/IP, UDP, ICMP

**Python Libraries**: Pandas, Numpy, Seaborn, Matplotlib

**Machine Learning**: Regression, Classification, Clustering

**Operating Systems**: Linux, Windows, Mac OS, Kali Linux.

**IDE Tools & Utilities**: Jupyter Notebook, Spyder, Ipython, Atom, Vim, Sublime, Pycharm, Git, SVN

**Selected Key Accomplishments**

✔Developed automation test scripts with improved execution process; reduced time by 30%, saving overall execution costs and time on Gryphon project.

✔Created a new framework for collecting and analyzing network data using Wireshark packet sniffer enabling the router to increase its

overall performance.

✔Setup improved UI automation framework by rewriting code; increased regression stability and reduced execution time.

✔Reduced the data extraction time by 50% on Cheric bank project.

**Professional Experience**

**Network Data and Test Engineer** • Gryphon Online Safety Inc • San Diego, CA Jan 2016–Present

Gryphon network router is an AI based router which will provide the customizable parental controls and provides Intrusion Detection System 24/7 to secure all the devices connected to it by using Machine Learning and Artificial Intelligence and will warn users and quarantine the devices when a device was compromised. It has a framework to collect the network data and process it to learn the behavior of various IoT devices.

* Designed and developed framework using Python and **Wireshark** libraries to analyze and process the network traffic.
* Developed API’s based on **SQLite** using Tshark, Scapy to collect, store and analyze the data
* Integrated the Data Processing framework with build system: **OpenWrt** and AWS Server.
* Responsible for simulating of IoT devices using **Raspberry Pi** and Linux platform for testing Intrusion Detection
* Created Hackable devices using Raspberry PI and Kali Linux for testing the framework developed.
* Responsible for integrating Intrusion Detection Framework with server and OpenWrt device.
* Developed Framework for visualizing the data using **Seaborn** and **Matplotlib**.
* Handle responsibilities of applying testing methodologies for testing various networking platforms and functionalities.
* Generated charts and drafted technical reports using Matplotlib and Seaborn.
* Developed automation scripts with **Rest Assured Framework** and **Hping3** for web services testing.
* Performed End-to-End Testing (E2E) on Data Framework using automated scripts.
* Assisted with debugging the Web Suite; used **SQL queries** in different contexts to verify the results and thoroughly debugged server logs using **Splunk Services**.
* Executed Continuous Integration of code and scripts using **Jenkins** and triggered the **Continuous Delivery** process using Jenkins build jobs.
* Prepared and reported execution status to senior management and product managers for every phase in the release.
* Played a key role in the triaging of production Incidents and execution of root cause analysis activities.
* Experience in monitoring tools such as such as **Wireshark** and **Tcpdump.**
* Following a Artificial Intelligence model, helping development by picking up **Machine Learning** work.

***Environment: Python, Wireshark, Tshark, hping3, Redmine, Pandas, Numpy, openWrt, PostgreSQL, Sqlite. Seaborn***

**PyUNIFAC** – City College of New York **[November 2013 –Dec2015]**

Python implementation of UNIFAC thermodynamic activity model - Models vapor-liquid and liquid-liquid equilibrium of multiple fluids based on chemical groups contained within the compounds

**Machine learning web application-** Web application using Flask and MongoDB, frontend designed with React - Allows users to upload data from Google spreadsheets, train machine learning models from Python’s Scikit-Learn module and use the models to generate predictions