Matthew Plascencia

714-760-1928 | plascencia.matt.31@gmail.com | linkedin.com/in/matthew-plascencia | github.com/tapatiohaxx

Education

Master of Science in Computer Science **Jan. 2023 – Present**
California State Polytechnic University-Pomona **Pomona, CA**

Bachelor of Science in Computer Science **Sep. 2017 – May 2021**
California State Polytechnic University-Pomona **Pomona, CA**

Experience

PolySec/Air Force Research Lab Drone Detection Researcher **Apr. 2023 – Present**
California State Polytechnic University-Pomona **Pomona, CA**

- Researched Orthogonal Frequency Division Multiplexing (OFDM) in DJI drones and leveraged findings to design novel experimental procedures to improve drone detection algorithms.
- Created and debugged python programs to parse and find correlations in OFDM features in DJI Air 2S, Air 2, and Phantom 3 drones to investigate which features are most varied in different drones' signals.
- Mentored undergraduate students on leveraging FieldFox analyzer and GNURadio/HackRF-based detection setup.

Clubs/Organizations

Director of Infrastructure Research - Forensics and Security Technology **Mar. 2023 – Present**
California State Polytechnic University-Pomona **Pomona, CA**

- Spearheaded a research team, delivering impactful insights into the intricate interplay between computer hardware and cloud technologies through engaging interactive presentations and practical hands-on labs.
- Directed production of yearly FAST CTF, ISSA LA CTFs, and SCaLE 20x CTF and contributed questions based on general forensics, mobile forensics, file system forensics, OSINT, Cryptography, and steganography.

Projects

Belkasoft iOS Forensics Course **Sep. 2023**

- Studied and performed iOS data extraction techniques such as agent-based acquisition, iCloud recovery and jailbreak acquisition to compare amounts of data produced by each technique.
- Analyzed knowledgeC.db utilizing SQL commands to discover how iOS stores app usage data, internet activity, device state, and other important user-related data such as music playback data.
- Conducted a practical case with iCloud backups, Signal data (with Apple Keychain) and WhatsApp data, and full iOS system dumps to observe iOS system structure and artifact locations.

Magnet Forensics Virtual CTF 2023 **May 2023**

- Built case against malicious actor using user profiles, Android device logs, and image/app databases gathered with Android Logs, Events and Protobuf Parser (ALEAPP) and Magnet Axiom.
- Found useful message and web history information in Android 12 file system through ALEAPP and Autopsy to build case against malicious actor.
- Documented and shared processes for solving CTF questions and setting up ALEAPP/Magnet Axiom in detailed writeup.

Licenses/Certifications

GIAC Foundational Cybersecurity Technologies (GFACT) **Issued Aug. 2023**

- Key Skills: SQL, BASH/PowerShell scripting, Memory/file system/email forensics. forensic acquisition, networking.

Technical Skills

Cyber security tools: ALEAPP, Autopsy, Belkasoft Evidence Center X, binwalk, CAINE iLEAPP, Kali Linux, Magnet Axiom, Sigma, Volatility Framework, Wireshark, Yara.
Programming Languages: C/C++, MySQL, Python.
Developer/Cloud Tools: AWS, Docker, Git, MS Azure, VS Code, Visual Studio.
Operating Systems: Linux, MacOS, Windows 10/11.