Packet Analysis with Python

Huntington
Welcome.®

Goals

- Understand the PCAP file format
- Use Python to process packet metadata and content
- Feed data into other Python-based tools for further analysis

Who Am I?

Not a developer!

- Someone told me Python would make my life easier
- I’ve been trying to escape ever since

Network Engineer

- Primary duties are troubleshooting and application performance assurance
- Python helps solve problems

Disclaimer

- I am not a developer
- My code is not perfect
- Take and use the ideas, not the code

Let's Dive into the Code!

Huntington
Welcome.®

Other Potential Applications

- Gather a single TCP connection into a list
    - Convert to a Numpy array for timing analysis and visualization
- Gather microsecond-level timestamp and packet length to identify micro-bursting
- In a decrypted stream, search for an HTTP X-Forwarded-For header to identify customer traffic behind a reverse proxy

Questions?

Thank you.