The research lab I work for at the Cyber Center for Security and Analytics at the University of Texas at San Antonio has given me the opportunity to work with a variety of industry standard tools and techniques. I spend most of my time working on fingerprinting traffic from Internet of Things devices across multiple protocols in order to baseline network activity, study malware interactions between IoT devices and traditional systems, and signature malicious IoT network traffic across these protocols. We have begun by studying TCP/IP, Bluetooth, and Zigbee network traffic with plans to look at other protocols later in the project. In order to facilitate this research, our lab has configured a spoke and hub network monitoring architecture consisting of multiple intrusion detection systems that analyze traffic between traditional honeypots and IoT devices. Tests are performed by connecting IoT devices to honeynets at geographically dispersed nodes. Data from each node is then streamed to a central repository at UTSA for analysis and categorization. Our primary goal is to identify malicious IoT network traffic and characterize existing or potential malware that operates across multiple protocols.