

I developed and evaluated Analytics, a tool that analyses packet data to learn information about network protocol formats. Analytics attempts to discover constants and enumeration fields among packet data, while providing visualization to aid analysts. My experiments on fixed length protocol headers show that the heuristics implemented for Analytics in detecting constants and enumeration fields are mostly accurate. It has an average accuracy in detecting constants of 76.8% and an average accuracy in detecting enumeration fields of 88.6%. As Analytics consists of heuristics to detect the targeted fields in network traces, it can also be applied onto proprietary or unknown protocols.

From my talk, audience can learn about network security and its significance. Poor network security can result in vulnerabilities in an organization, which may result in commercial espionage, the leakage of company secrets, or the control of computers connected to the network to perform illegal activities. Audience can also benefit from my talk by learning about Deep Packet Inspection, a common process used in large organizations to maintain network security and prevent the transfer of malicious data through a network. Experts in the field can appreciate the tool, 'Analytics', that demonstrates the use of Python in garnering information about unknown network protocol formats.