Analyzing PCAPs

Mission: Find all the malicious IP addresses

The mission is to write a python script using the various modules such as Scapy for analyzing provided PCAP file and generate a new CSV report with two columns of found IP addresses and their maliciousness.

Short Definitions

- Scapy - a standalone tool as well as a Python module that allow us to create a network packet from scratch regarding the protocols.
- PCAP - a product of network packet capture done via wireshark or other sniffing tool (scapy able to do so as well)
- CSV - a comma separated document that could be loaded into Excel for further reporting

Suggested Steps

1. Go over the Scapy notebook
2. Run over basic Scapy commands and get familiar with the module
3. Get familiar with https://www.abuseipdb.com/ API and its workflow
4. Be strong! and don't giveup!