**PcapXray Design Specification**

**Goal:**

* Given a Pcap File, plot a network diagram displaying hosts in the network, network traffic, highlight important traffic and Tor traffic as well as potential malicious traffic including files involved in the communication.

**Problem:**

* Investigation of a Pcap file takes a long time given initial glitch to start the investigation
  + Faced by every forensics investigator and anyone who is analyzing the network

**Solution:**

* Make a network diagram with the following features from a Pcap file
  + **Tool Highlights:**
    - Network Diagram – Summary Network Diagram of full network
    - Specific Host Diagram
      * Traffic with Server Details
      * Tor Traffic
      * Files Exchanged
      * Possible Malicious traffic
      * Device Details and Possible Social Engineering of Host

**Components:**

* **Mandatory:**
  + Network Diagram + Specific Host Diagram
  + Device Details and Analysis
  + Malicious Traffic Identification
  + Tor Traffic
  + GUI – a gui with options to upload pcap file and display the network diagram
* **Optional but Useful:**
  + Files Exchanged
  + Server Details in traffic

**Block Diagram:**

**Flow Diagram:**