The world being represented is an application capable is gathering network traffic data from a network security device (such as a router or firewall) and parsing through the traffic in real time. This is known in the real world as a network Intrusion Detection Service (IDS) tool The application will then be able to use a set of sensors to flag the data as either benign or malicious. The traffic captured is benchmarked against a time stamp (known as the system time). The traffic consists of a set of attributes under three categories which map the ISO layers 2-4:

1. Frame; which contains attributes representing the data required for node to node data transfer between a network. The attributes include interface id (the network interface the traffic arrived at), arrival time, Frame Number, Frame length, frame type (ethernet, wireless etc.)
2. Ethernet: this contains attributes representing the data required for addressing, routing and traffic control between computer networks. It includes data like the Destination and Source address and network protocol used
3. Transport: this contains attributes representing the data required for transferring data while maintaining the quality of service functions. It includes flags designed to provide connection (with recovery) or connectionless oriented data transfers. Some attributes include: TTL, Protocol, Total length, Source Address, Destination Address.
4. User Datagram: This contains attributes to identify where the processing on the host and remote computer will be. It contains the source port, destination port and length

The application allows the administrator to pin network packets to a network based on the CIDR reported as the source IP. For example, the administrator might assign 10.12.0.0/16 range as belonging in their DMZ. However, they can also specify that 10.12.135.0/24 belongs to the Shanghai DMZ.

Once the data is gathered the application contains a list of sensors which can mark data transfers as being benign or malicious based on a set of attributes the sensor contains. For example, a sensor could detect connection to a botnet using a list of known malicious IP address (Internet Protocol address). If the Transport or Ethernet attributes contains an IP address in the backlist, then the sensor will flag it as malicious. Off importance if that the sensor can flag traffic by specifying a range of packets or one. One of more sensors may flag a traffic based on packet and network. Conversely, any given traffic packet might not be flagged by any sensor at all.

Also, within the application is a set of response that the sensor can trigger if it finds a match from the network traffic. For example, the sensor that filters the traffic for connections to known malicious IP can consist of several response actions such as add the traffic Id to a pre-made report template, fire an email send a notification to the application. The response is also optionally limited with a threshold given a timespan. For example, the response may be limited not to fire more than 30 times (the threshold) in a 30-minute (timespan) interval.

Steps:

1. First once I used Docker to build an image for my application.
2. Then I built my docker image using the following command: