Notes explaining project:

The aim of the project is to integrate Zeek with a Ryu controlled virtual network generated by Mininet.

Zeek is an open-source network security monitor that implements security functionality like examining packets and determining if there is malicious behaviour from the packet sender, quarantining hosts, etc. Through the NetControl framework (basically like a package for zeek), it can connect to Ryu and control our network, sending commands to Ryu which sends commands to the switch etc.

Mininet is a virtual network simulator that can be used as either a command line tool, or in a programmatic way. You can generate custom network topologies with mininet using its python API.

Ryu is a software-defined network controller. With it you can implement specific functionality to control switches in mininet. In the example ryu script we run, I implement a simple learning switch that associates MAC addresses with its output interfaces to more efficiently forward packets. It also blocks communications between hosts 2 and 3 as a learning exercise.

In the fresh_install.sh script, I use the following mininet command to create a custom topology with 3 hosts connected to a switch

```
sudo mn --controller=remote --topo=single,3 --switch=ovsk,protocols=OpenFlow10 --mac &
```

The —controller=remote flag sets the network controller (which implements the OpenFlow protocol) to remote, meaning a controller external to mininet.

The following command then runs our Ryu controller defined in our custom script and connects it to mininet.

ryu-manager ./sdn/ss13_filter.py

Basically the next thing to do in the project is to examine the code at

https://github.com/zeek/zeek-netcontrol/tree/master/openflow

which implements an integration between ryu and zeek and see if I can

make my own version of it...

Good luck bro