

1) By using

<http://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=get&target=http.cap> file, create a csv file. The format of the csv file should like the below:

```
source,target,value
```

Source: source ip

Target: destination ip

value: strength of the link between source and destination (by looking at the number of connections between source and destination you may define a values, the more connection the higher value you may define)

2) By using the above csv file, create a forced directed graph. You may use d3.js. An HTML file should be created (display.html) that is displaying nodes (IP addresses) and connections between them.

3) Write an IRC handler that reads a pcap and understands it and parse its information. The handler should be a class and the usage example should be demonstrated with the pcap sample.

4) Write a DNS handler and test it for

<http://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=get&target=dns-remoteshell.pcap> The handler should undertand the DNS anomaly and display the results.

Python is the preferred coding language. You may use whatever plugins you want. Put your source code to your Github acoounts and send their links.