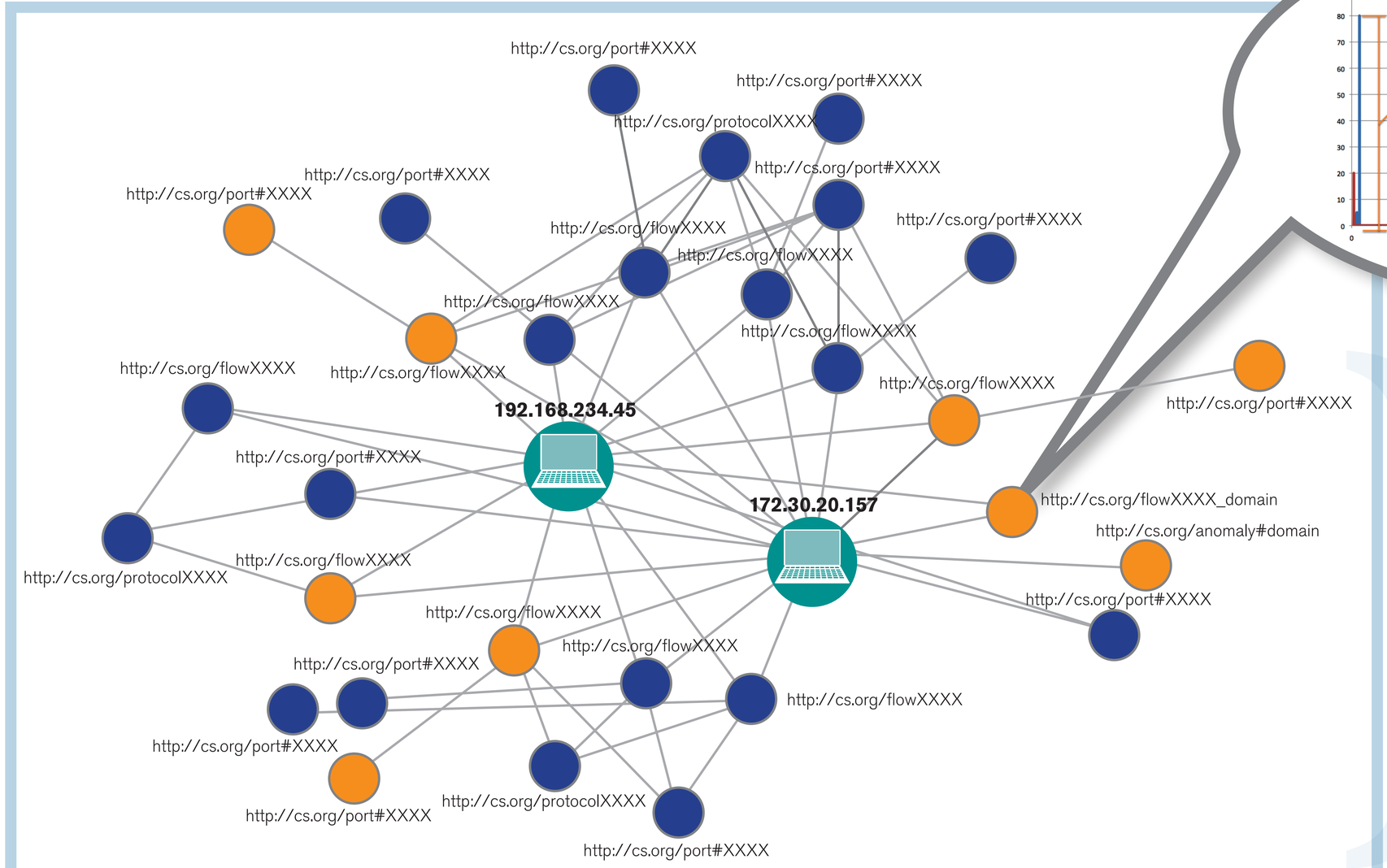
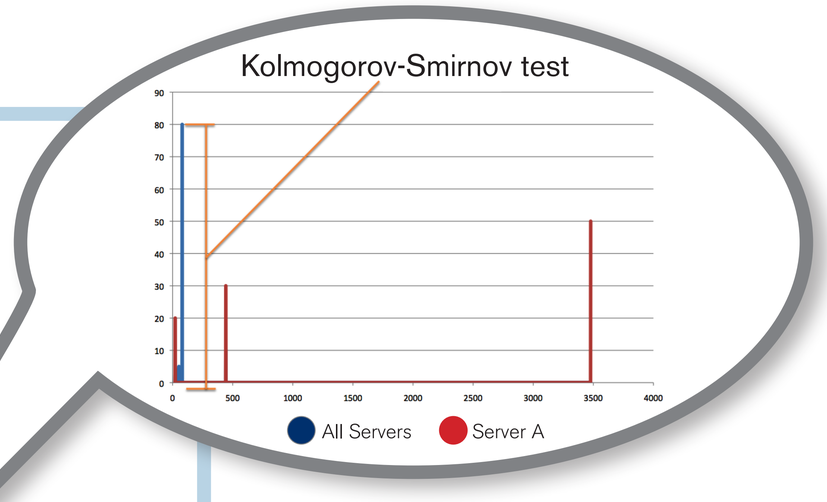
Discovering unknown network activity using graphs and computer network data





Prioritized Anomaly List

ip1	ip2
http://cs.org/ipv4#172.31.21.12	http://cs.org/ipv4#172.30.74.167
http://cs.org/ipv4#172.30.20.157	http://cs.org/ipv4#192.168.234.45
http://cs.org/ipv4#172.31.21.12	http://cs.org/ipv4#172.30.74.189
http://cs.org/ipv4#172.30.22.166	http://cs.org/ipv4#157.55.130.152
http://cs.org/ipv4#172.30.19.126	http://cs.org/ipv4#192.168.234.45
http://cs.org/ipv4#172.30.22.166	http://cs.org/ipv4#157.56.52.18
http://cs.org/ipv4#172.30.22.166	http://cs.org/ipv4#157.55.130.158
http://cs.org/ipv4#192.168.233.237	http://cs.org/ipv4#213.199.179.142
http://cs.org/ipv4#172.30.22.166	http://cs.org/ipv4#91.190.216.26
http://cs.org/ipv4#172.30.22.166	http://cs.org/ipv4#157.55.56.148
http://cs.org/ipv4#172.30.22.166	http://cs.org/ipv4#192.168.234.45
http://cs.org/ipv4#192.168.233.237	http://cs.org/ipv4#157.55.56.160
http://cs.org/ipv4#192.168.233.221	http://cs.org/ipv4#74.125.142.125
http://cs.org/ipv4#192.168.233.221	http://cs.org/ipv4#209.85.225.125
http://cs.org/ipv4#192.168.233.221	http://cs.org/ipv4#10.1.1.233
http://cs.org/ipv4#192.168.233.237	http://cs.org/ipv4#24.62.201.161
http://cs.org/ipv4#192.168.233.237	http://cs.org/ipv4#157.55.130.152
http://cs.org/ipv4#192.168.233.237	http://cs.org/ipv4#192.168.209.56
http://cs.org/ipv4#192.168.233.237	http://cs.org/ipv4#91.190.216.26
http://cs.org/ipv4#192.168.233.237	http://cs.org/ipv4#157.55.130.158
http://cs.org/ipv4#192.168.233.237	http://cs.org/ipv4#157.55.56.148

How to use broad and deep computer network data (netflow, web activity, and DNS requests), statistics, and graph algorithms to automatically identify and prioritize anomalous network activity.

Eric Dull, Technical Director, YarcData

FloCon 2014
January 13-16, 2014 | Charleston, South Carolina
YarcData
Getting to **Eureka!** faster™