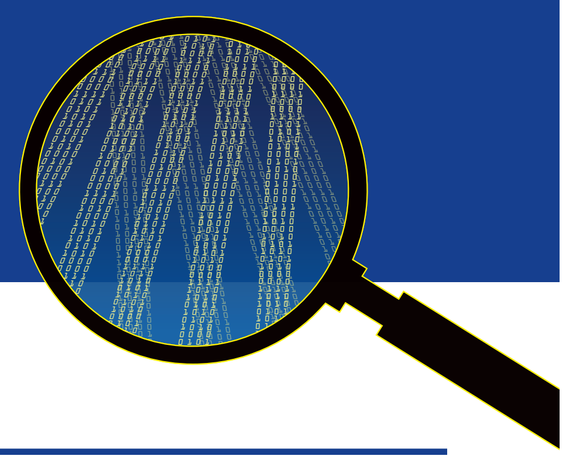
FloCon®2014



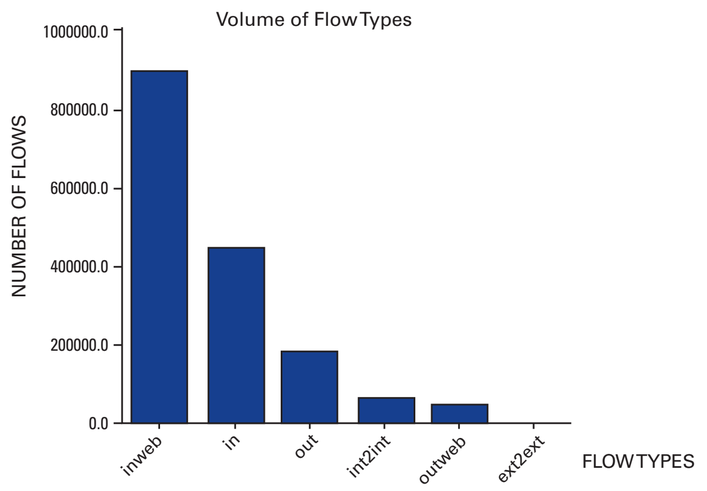
Visualization of Network Flow Data

Network flow data has very low information content; consequently you need a lot of data, or need to know something specific about it. We introduce three methods or reasons to visualize such data: Descriptive, Retrospective Analysis and exploratory.

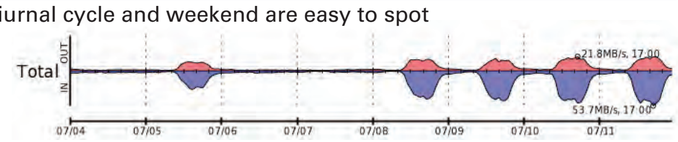
Simplified Network Flow Record						
sTime	eTime	sIP	dIP	Sport	Dport	Proto
Pkts	Bytes	Type	Sensor			
Flags	iFlags	sFlags	Att	AppLbl		

Describe

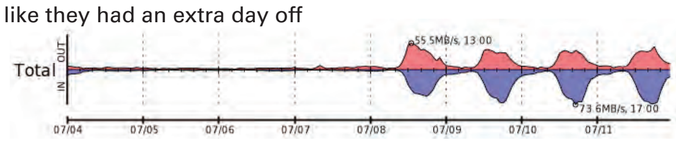
What's happening? What's typical? See the big picture.



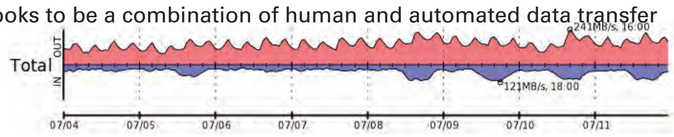
The diurnal cycle and weekend are easy to spot



Looks like they had an extra day off

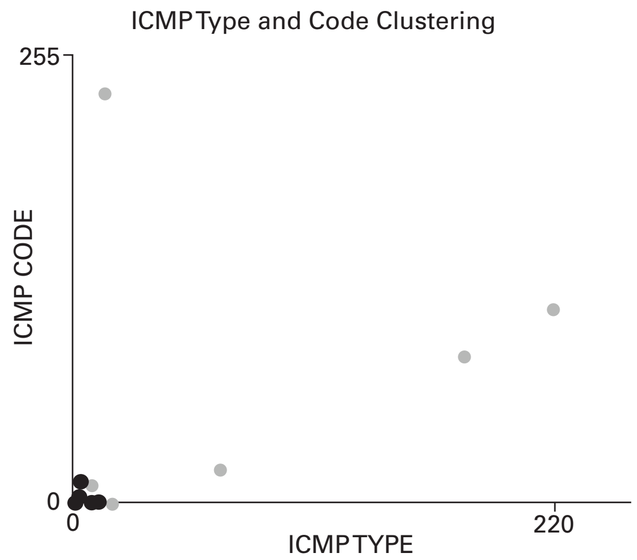


This looks to be a combination of human and automated data transfer



Analyze

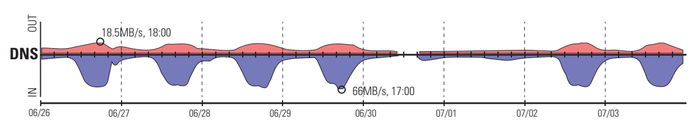
Something happened. Describe it. Who, what, where, when…? Profile a network or a host IP

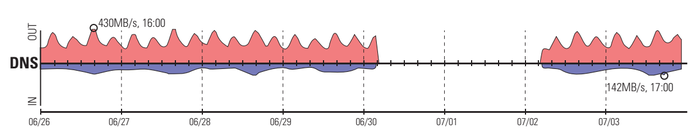


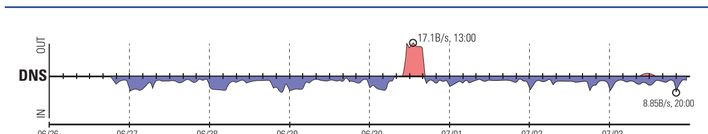
Explore

I can describe Activity X in network terms, can I find instances of it occurring? Look for anomalies

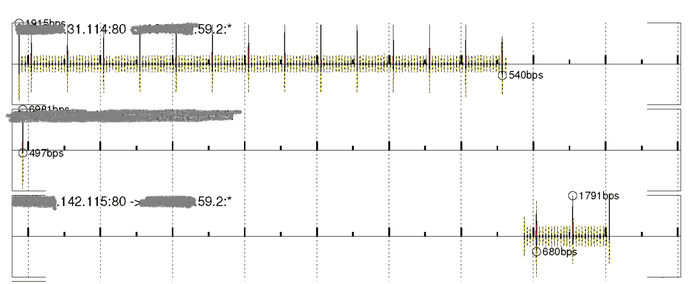
Were there any visible effects of the power failure?







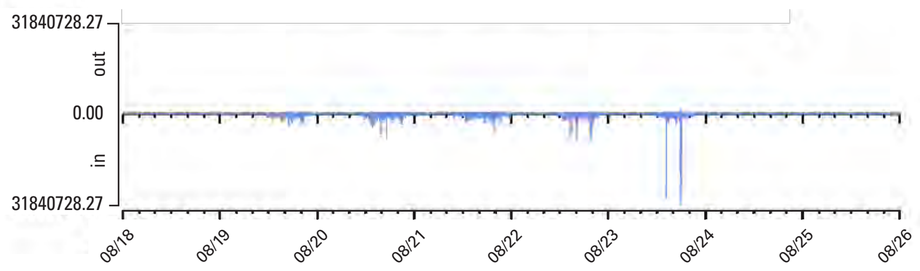
Can we find beaconing to C2 servers?



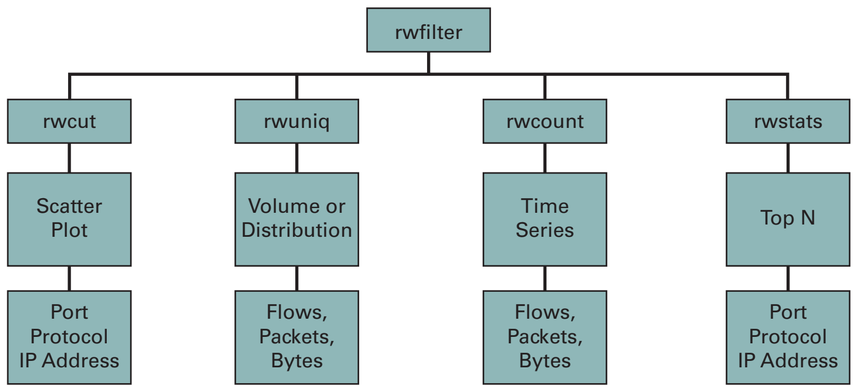
Generic data preparation process

SiLK and Rayon data preparation process

Youtube traffic: one sensor eight days



How to get the data you need with SiLK



http://www.cert.org/flocon