

Applied Detection and Analysis Using Network Flow Data

Chris Sanders and Jason Smith
TAP Intel-Based Detection
Mandiant, a FireEye Company

Chris Sanders

- Christian & Husband
- Kentuckian and South Carolinian
- MS, GSE, et al.
- Non-Profit Director
- BBQ Pit Master



Jason Smith

- Kentuckian
- Car Aficionado
- Raspberry Pi enthusiast
- Junkyard Engineer



MIRcon.
2014

3

Applied Network Security Monitoring



“This book should be required reading for all intrusion analysts and those looking to develop a security monitoring program.”

“Written by analysts, for analysts.”

- Amazon Reviewers

MIRcon.
2014

4

Agenda

Flow Data!

- Why it's important
- How you can collect it
- What you can do with it
- Tools that can help

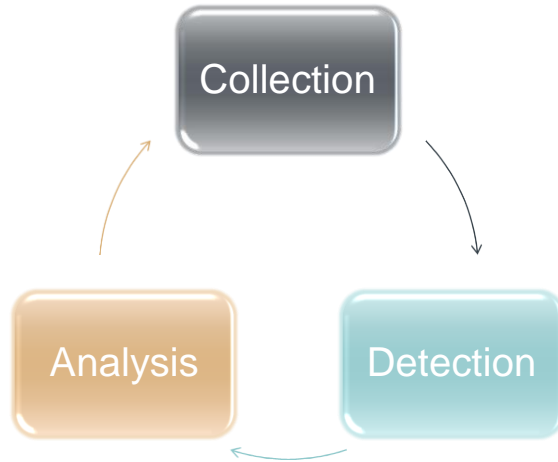
“Why/How to use Flow Data in NSM/IR”

Network Security Monitoring

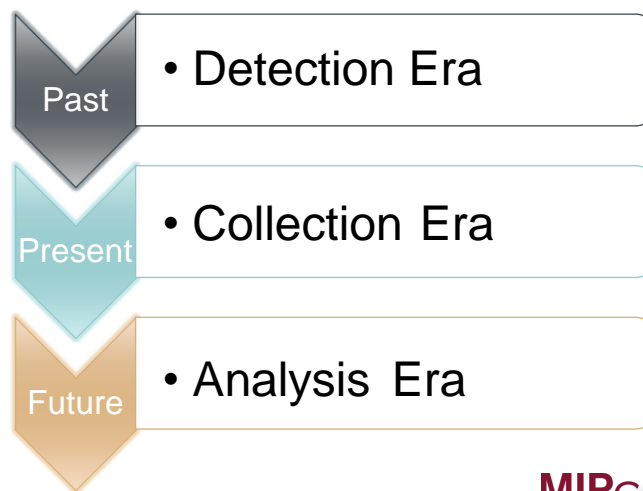
- The collection, detection, and analysis of network security data.
- The goal of NSM is escalation, or to declare that an incident has occurred so that incident response can occur.



The NSM Cycle



Evolution of NSM Emphasis



NSM/IR Challenges of the Present

We All Want Full PCAP...

- Collection
 - Easy to Capture / Filter Stream Data
- Detection
 - Major Detection Tools are PCAP Oriented
- Analysis
 - Gives us Who, Where, When, and What

NSM/IR Challenges of the Present

But, It's not Feasible for Every Goal...

- Collection
 - Not Scalable for Extended Retention
- Detection
 - Not Ideal of Hunting / Rapid Pivoting
- Analysis
 - Not a Great Starting Point

Full PCAP vs. Flow Data



PCAP Data

NEXTEL Account name: [REDACTED] Page 13
Account number: [REDACTED]
Statement date: May 23, 2003
Billing period: April 19 - May 18, 2003

continued...

Telecommunications Services Call Detail

Item #	Date	Time	Call To	Number Called	Sec	Port	Min	Sec	Usage	Long Distance	Total Charges
10	May 04	04:00	PM	CLEVELAND, OH	216-407-0702	SP	PU	1:00	0:00	0:00	0.00
11	May 04	08:00	PM	COLUMBIANA, OH	440-298-0800	SP	PU	1:00	0:00	0:00	0.00
12	May 04	08:00	PM	CLYDE, OH	440-507-0400	SP	PU	2:00	0:00	0:00	0.00
13	May 04	07:00	PM	CLEVELAND, OH	216-321-1900	SP	PU	1:00	0:00	0:00	0.00
14	May 04	10:00	PM	CLEVELAND, OH	760000	SP	PU	1:00	0:00	0:00	0.00
15	May 04	10:10	PM	CLEVELAND, OH	760000	SP	PU	1:00	0:00	0:00	0.00
16	May 04	02:00	PM	PARSONS, PA	800-400-0400	PP	PU	2:00	0:00	0:00	0.00
17	May 13	06:07	PM	CLEVELAND, OH	216-700-1000	SP	PU	1:00	0:00	0:00	0.00
18	May 13	07:17	PM	CLEVELAND, OH	216-700-1000	SP	PU	1:00	0:00	0:00	0.00
19	May 14	06:01	PM	PARSONS, PA	800-400-0400	PP	PU	1:00	0:00	0:00	0.00
20	May 14	06:03	PM	PARSONS, PA	800-400-0400	PP	PU	2:00	0:00	0:00	0.00
21	May 14	08:00	PM	TALL, PA	800-800-7000	PP	PU	1:00	0:00	0:00	0.00

Flow Data

Flow Data

- Often Called Flow / Session / NetFlow
- Summary of Network Communications
- Aggregated Record of Packets
- Gives Us Who, Where, When
- Based on the 5-tuple + Timing/Data Stats

Source IP	Source Port	Dest IP	Dest Port	Protocol
192.168.5.1	48293	8.8.8.8	53	UDP

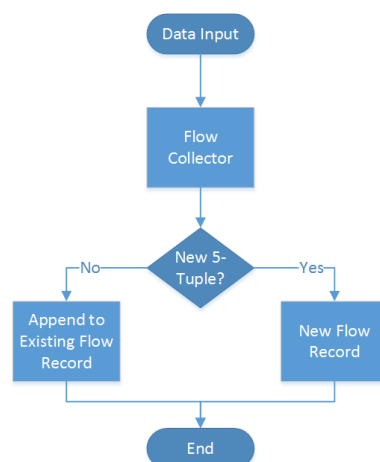
Start Time	End Time	Bytes
2014/09/22T00:03:58.756	2014/09/22T00:04:58.756	76

Flow Data Example

sTime	sIP dPort	dIP dPort pro bytes
2014/09/22T00:03:58.756	10.10.120.1 53	10.1.179.5 53 17 72
2014/09/22T00:03:58.999	10.10.120.1 53	10.1.188.5 53 17 89
2014/09/22T00:08:59.012	10.10.120.1 53	10.1.179.5 53 17 72
2014/09/22T00:08:59.466	10.10.120.1 53	10.1.188.5 53 17 89
2014/09/22T00:03:58.756	10.10.120.1 53	10.1.179.5 53 17 72
2014/09/22T00:03:58.999	10.10.120.1 53	10.1.188.5 53 17 89
2014/09/22T00:08:59.012	10.10.120.1 53	10.1.179.5 53 17 72
2014/09/22T00:08:59.466	10.10.120.1 53	10.1.188.5 53 17 89

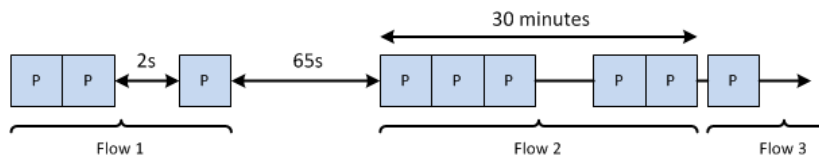
Building Flow Records

- Records are Defined by Unique 5-tuples
- Data is added to the 5-tuple Record until a termination condition is met.



Flow Record Termination Conditions

- Natural Timeout
 - End of communication per protocol (ex. TCP RST/FIN)
- Idle Timeout
 - No data received for 30 seconds
- Active Timeout
 - Thirty minute max timeout (configurable)



Collection with Flow Data

Generating Flow Data

- Generation
 - Routers
 - Sensors
 - Fprobe
 - YAF
- Multiple Types:
 - NetFlow (v5,v9)
 - IPFIX
 - jFlow
 - More...

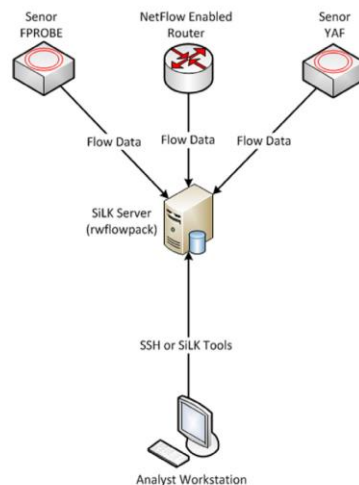
Collecting Flow Data

- Popular Platforms
 - Argus
 - + Reliable + Fast Collection
 - Not Well Supported
 - NFDump
 - + Easy to Setup and Use
 - Not in Wide Use
 - SiLK
 - + Exceptional Analysis Tools
 - More Involved Setup

SiLK

- The System for Internet-Level Knowledge
- CERT NetSA Team
- Two Major Components:
 - Packing Suite
 - Collection and parsing of flow data
 - Analysis Suite
 - Filter, display, sort, count, group, mate, and more
- Excellent Documentation & Community
 - <https://tools.netsa.cert.org/silk/docs.html>

SiLK Collection Architecture



SiLK – What You Need

- Flow Sources
 - Hardware: Routers, Switches
 - Software: YAF, fprobe
- SiLK Server
 - Rwflowpack
 - Will also have SiLK analysis suite installed
- Analyst Workstation
 - Access SiLK server directly
 - Locally mirrored database

SiLK – Analysis Suite

- rfilter - Filters through data based on conditions.
- rwcut - Converts flow binary data to a human readable format.
- rwstats - Generates statistics from flow data
- rwcoun - Summarizes total network traffic over time

SiLK Analysis – rfilter / rwcut (1)

- Display all records from the beginning the current day until the current time:

```
rfilter --type=all --proto=0-255 --pass=stdout | rwcut
```

sIP	dIP	sPort	dPort	proto	packets	bytes	flags	sTime	duration	eTime	sen
197.9.246.221	182.14.164.4	35811	50066	6	3	132	FS A	2014/05/13T10:00:02.043	0.225	2014/05/13T10:00:02.268	51
197.9.246.221	182.14.164.4	21	50065	6	14	853	FS PA	2014/05/13T10:00:01.304	1.982	2014/05/13T10:00:03.286	51
68.30.155.170	182.82.134.177	53627	3001	6	7	770	FS PA	2014/05/13T10:00:03.430	0.187	2014/05/13T10:00:03.617	51
197.9.246.221	182.14.164.4	35824	50068	6	3	132	FS A	2014/05/13T10:00:04.361	0.239	2014/05/13T10:00:04.600	51
68.30.155.170	182.82.134.177	53628	3003	6	7	770	FS PA	2014/05/13T10:00:05.198	0.190	2014/05/13T10:00:05.388	51
68.30.155.170	182.82.134.177	53630	3001	6	7	770	FS PA	2014/05/13T10:00:06.081	0.195	2014/05/13T10:00:06.276	51
197.9.246.221	182.14.164.4	35171	50070	6	3	132	FS A	2014/05/13T10:00:06.670	0.206	2014/05/13T10:00:06.965	51
68.30.155.170	182.82.134.177	53631	3003	6	8	1081	FSRPA	2014/05/13T10:00:06.456	0.651	2014/05/13T10:00:07.107	51
68.30.155.170	182.82.134.177	53629	3002	6	423	468072	FSRPA	2014/05/13T10:00:05.521	2.454	2014/05/13T10:00:07.975	51
68.30.155.170	182.82.134.177	53629	3002	6	483	462473	FSRPA	2014/05/13T10:00:05.522	2.453	2014/05/13T10:00:07.975	51
197.9.246.221	182.14.164.4	21	50069	6	13	812	S PA	2014/05/13T10:00:05.944	2.049	2014/05/13T10:00:07.993	51
197.9.246.221	182.14.164.4	21	50069	6	1	40	F A	2014/05/13T10:00:07.994	0.000	2014/05/13T10:00:07.994	51
5.47.194.56	182.140.208.205	22	64210	6	45	7317	S PA	2014/05/13T10:00:07.773	1.421	2014/05/13T10:00:09.194	51
5.47.194.56	182.140.208.205	22	64210	6	1	40	F A	2014/05/13T10:00:09.195	0.001	2014/05/13T10:00:09.196	51
197.9.246.221	182.14.164.4	35802	50072	6	3	132	FS A	2014/05/13T10:00:09.044	0.229	2014/05/13T10:00:09.273	51
197.9.246.221	182.14.164.4	35806	50074	6	3	132	FS A	2014/05/13T10:00:11.382	0.234	2014/05/13T10:00:11.616	51
197.9.246.221	182.14.164.4	21	50073	6	13	813	FS PA	2014/05/13T10:00:10.450	1.982	2014/05/13T10:00:12.632	51
197.9.246.221	182.14.164.4	21	50073	6	1	40	F A	2014/05/13T10:00:12.634	0.002	2014/05/13T10:00:12.636	51
197.9.246.221	182.14.164.4	35176	50076	6	3	132	FS A	2014/05/13T10:00:13.787	0.231	2014/05/13T10:00:13.938	51
197.9.246.221	182.14.164.4	21	50077	6	13	812	FS PA	2014/05/13T10:00:15.314	1.997	2014/05/13T10:00:17.311	51
197.9.246.221	182.14.164.4	35160	50080	6	3	132	FS A	2014/05/13T10:00:18.470	0.229	2014/05/13T10:00:18.699	51
6.128.17.150	11.237.137.249	54969	5900	6	2	84	SR	2014/05/13T10:00:04.355	14.655	2014/05/13T10:00:19.810	51
197.9.246.221	182.14.164.4	35800	50082	6	3	132	FS A	2014/05/13T10:00:21.194	0.233	2014/05/13T10:00:21.427	51
197.9.246.221	182.14.164.4	21	50081	6	14	852	FS PA	2014/05/13T10:00:20.324	2.141	2014/05/13T10:00:22.465	51
143.141.15.64	182.82.134.205	8443	51142	6	4	179	FS PA	2014/05/13T10:00:22.712	0.051	2014/05/13T10:00:22.763	51
143.141.15.64	182.82.134.205	8443	51143	6	11	3850	FS PA	2014/05/13T10:00:22.763	1.302	2014/05/13T10:00:24.154	51

SiLK Analysis – rfilter / rwcut (2)

- Display all records of communication to or from Chinese IP addresses over a specific week to one local CIDR range:

```
rfilter --type=all --start-date=2014/08/01 --end-date=2014/08/07 --any-address=192.168.1.0/24 --any-cc=cn --pass=stdout | rwcut --fields=sTime,sIP,dIP,sPort,dPort,type
```

sTime	sIP	dIP	sPort	dPort	type
2014/08/05T15:54:50.990	10.106.123.45	10.107.173.196	28993	41142	in
2014/08/05T15:54:50.992	10.194.186.42	172.28.239.102	41142	28993	out
2014/08/05T18:04:00.090	10.122.74.199	10.31.10.21	1026	41142	in
2014/08/05T23:50:48.570	10.52.111.14	10.138.232.188	40357	41142	in
2014/08/05T23:58:01.418	10.117.48.59	10.24.175.71	53312	41142	in
2014/08/05T23:50:48.572	10.73.176.195	10.10.20.112	41142	40357	out
2014/08/05T23:58:01.475	10.55.121.43	10.165.47.26	41142	53312	out
2014/08/06T00:13:57.692	10.104.43.101	10.127.158.111	13202	41142	in
2014/08/06T00:18:30.596	10.142.187.222	10.71.237.199	51807	41142	in
2014/08/06T00:24:41.160	10.134.111.247	10.210.221.167	164330	41142	in

SiLK Analysis – rwstats (1)

- Display statistics for the total amount of bytes transferred by protocol (top 10):

```
rwfilter --type=all --proto=0-255 --pass=stdout |  
rwstats --top --count=10 --fields=proto --  
value=bytes
```

```
INPUT: 7671365 Records for 7 Bins and 1880722375406 Total Bytes  
OUTPUT: Top 10 Bins by Bytes  
pro|      Bytes|    %Bytes|  cumul_%|  
6|      1876692757588| 99.785741| 99.785741|  
17|      3886949450| 0.206673| 99.992414|  
1|      69185319| 0.003679| 99.996093|  
47|      40843957| 0.002172| 99.998265|  
50|      31424357| 0.001671| 99.999935|  
41|      1144367| 0.000061| 99.999996|  
2|      70368| 0.000004| 100.000000|
```

SiLK Analysis – rwstats (2)

- Show the top 10 sip,dip pairs for valid conversations (top 10)

```
rwfilter --type=all --proto=0-255 --packets=4, --  
pass=stdout | rwstats --top --count=10 --  
fields=sip,dip --value=bytes
```

```
INPUT: 3553669 Records for 210934 Bins and 1880090680938 Total Bytes  
OUTPUT: Top 10 Bins by Bytes  
sip|      dip|      Bytes|    %Bytes|  cumul_%|  
182.82.172.111| 182.140.188.64| 219038598507| 11.650427| 11.650427|  
182.140.188.64| 182.82.26.133| 188205311455| 10.010438| 21.660865|  
182.82.3.85| 182.140.188.64| 180386700023| 9.594574| 31.255440|  
182.140.188.64| 182.82.3.85| 163207001357| 8.680805| 39.936245|  
11.237.171.87| 182.140.188.102| 158910367747| 8.452271| 48.388516|  
182.82.26.133| 182.140.188.64| 135227063103| 7.192582| 55.581098|  
182.82.145.235| 182.140.188.64| 119072866667| 6.333358| 61.914456|  
182.140.188.64| 182.82.145.235| 117393912025| 6.244056| 68.158511|  
11.237.171.166| 182.140.188.111| 90192333665| 4.797233| 72.955745|  
97.125.231.85| 11.237.224.220| 79984274054| 4.254277| 77.210022|
```

SiLK Analysis – rwstats (3)

- Show the top 10 outbound destination country codes by records:

```
rwfilter --type=out,outweb --proto=0-255 --  
pass=stdout | rwstats --top --count=10 --fields=dcc
```

```
INPUT: 7125124 Records for 147 Bins and 7125124 Total Records  
OUTPUT: Top 10 Bins by Records
```

dcc	Records	%Records	cumul_%
us	2677276	37.575150	37.575150
cn	2234597	31.362219	68.937369
id	834469	11.711642	80.649010
in	327519	4.596678	85.245688
ar	313590	4.401187	89.646875
jp	231349	3.246947	92.893822
gb	38085	0.534517	93.428339
de	36410	0.511009	93.939348
cl	32304	0.453382	94.392729
my	28288	0.397018	94.789747

SiLK Analysis – Real World Examples

- Rwstats to discover potential ZeroAccess victims

```
rwfilter --type=all --dport=16464,16465,16470,16471 --  
pass=stdout | rwstats --top --fields=sip --  
value=distinct:dcc --threshold=3
```

```
INPUT: 272 Records for 1 Bin  
OUTPUT: Top 1 bins by dcc-Distinct (threshold 3)  
sip|dcc|%dcc-Disti| cumul_%|  
192.168.106.131| 52| ?| ?|
```

SiLK Analysis – Real World Examples

- Discovering outbound data to applications using nonstandard ports.

```
rwfilter Sampledata/sample.rw \  
--plugin=app-mismatch.so \  
--type=out,outweb --proto=6 \  
--sport=1024- \  
--packets=4- \  
--flags-initial=S/SURFPACE \  
--pass=stdout | \  
rwstats --fields=application,dport --count=100 \  
--distinct:dport
```

INPUT: 3420 Records for 4 Bins
OUTPUT: Top 100 Bins by dPort-Distinct

appli	dPort-Dist	%dPort-Dist	cumul_
80	23	?	?
22	5	?	?
21	2	?	?
5222	1	?	?

Collecting Intelligence Data

- Friendly Intelligence Gathering
- Identify Services on the Network
- Identify Normal Behaviors of Hosts
- Identify “Friends and Family”
 - Friends: Who a host communicates with outside the network
 - Family: Who a host communicates with inside the network

Identifying Services

- Identify SSH Servers

```
rwfilter --type=out --protocol=6 --packets=4- -  
-ack-flag=1 --sport=22 --pass=stdout | rwcut --  
fields=sip
```

- Identify Web Servers

```
rwfilter --type=outweb --protocol=6 --  
packets=4- --ack-flag=1 --sport=80,443,8080 --  
pass=stdout | rwcut --fields=sip
```

Identifying Friends and Family

- Identify Friends

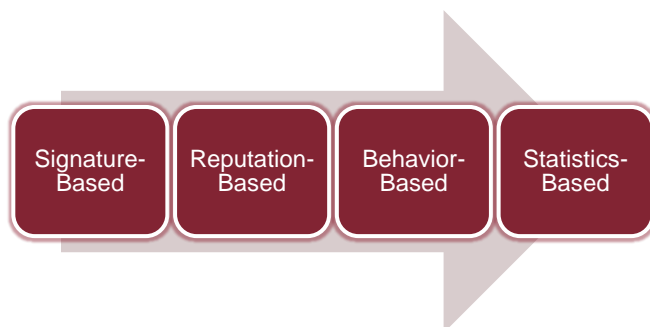
```
rwfilter --type=out,outweb --  
saddress=192.168.1.1 --pass=stdout |  
rwfilter --input-pipe=stdin --  
dcidr=192.168.0.0/24 --fail=stdout
```

- Identify Family

```
rwfilter --type=out,outweb --  
saddress=192.168.1.1 --pass=stdout |  
rwfilter --input-pipe=stdin --  
dipset=local --fail=stdout
```


Detection with Flow Data

Flow for Detection

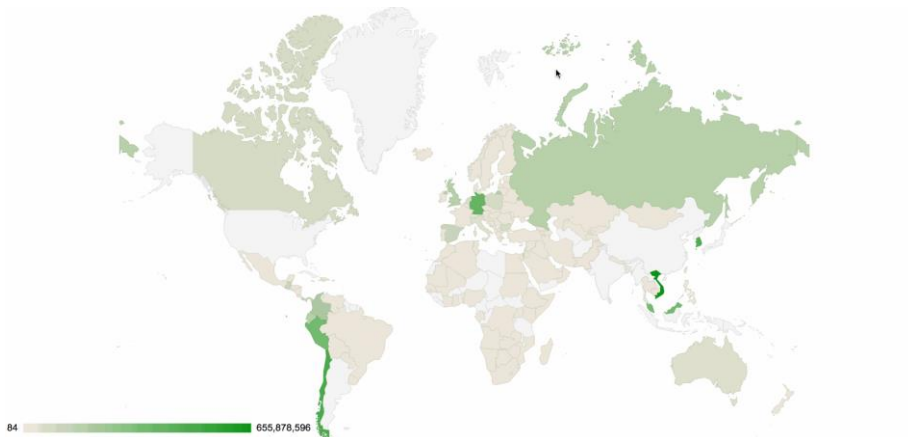


FlowPlotter

- Generates Visualizations from the Output of Flow Tools
- Useful for Detection-Oriented Statistics
- Written in BASH – Flexible/Tweakable/Minimal
- Free/Open Source - Maintained in GitHub
- Browser Independent

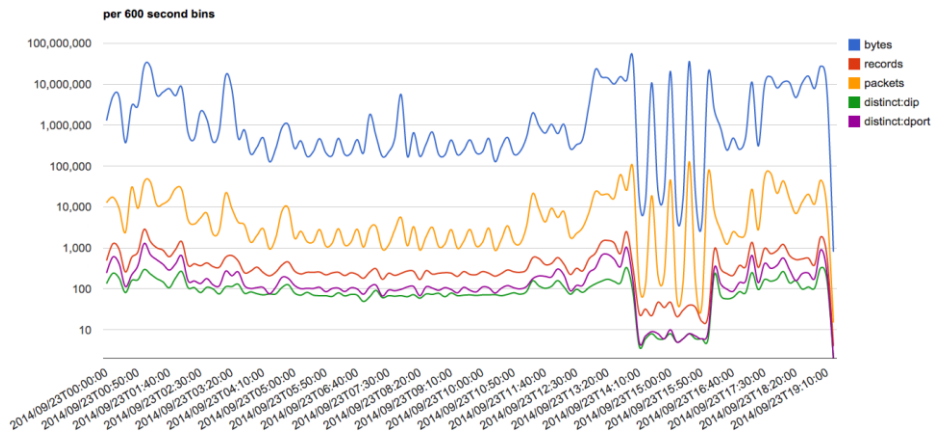
FlowPlotter - GeoMap

- `rwfilter ../Sampledata/sample.rw --dcc=us,cn,-- --fail=stdout |
./flowplotter.sh geomap dcc bytes > geomap.html`



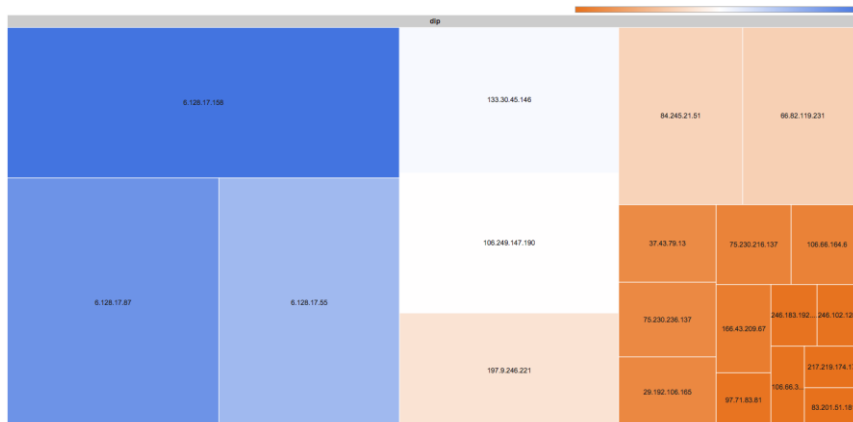
FlowPlotter - LineChart

- `rwfilter --type=all --proto=0-255 --pass=stdout | ./flowplotter.sh linechart 600 bytes > linechart.html`



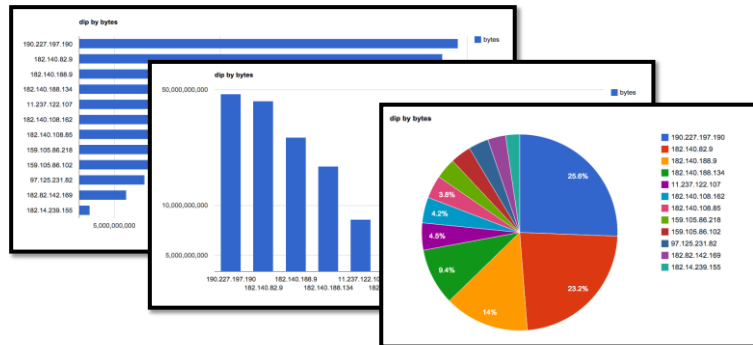
FlowPlotter - TreeMap

- `rwfilter ../Sampledata/sample.rw --sport=1025- --dport=1025- --proto=0- --type=out --pass=stdout | ./flowplotter.sh treemap dip records > treemap.html`



FlowPlotter - Pie/Bar/Column Chart

- rwfilter ../Sampledata/sample.rw --sport=1025- --dport=1025- --proto=0- --type=all --pass=stdout | ./flowplotter.sh piechart dip bytes > piechart.html

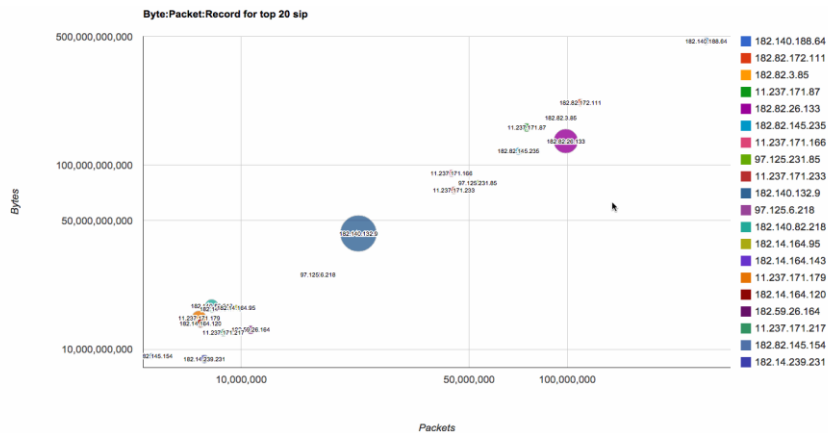


MIRcon 2014

39

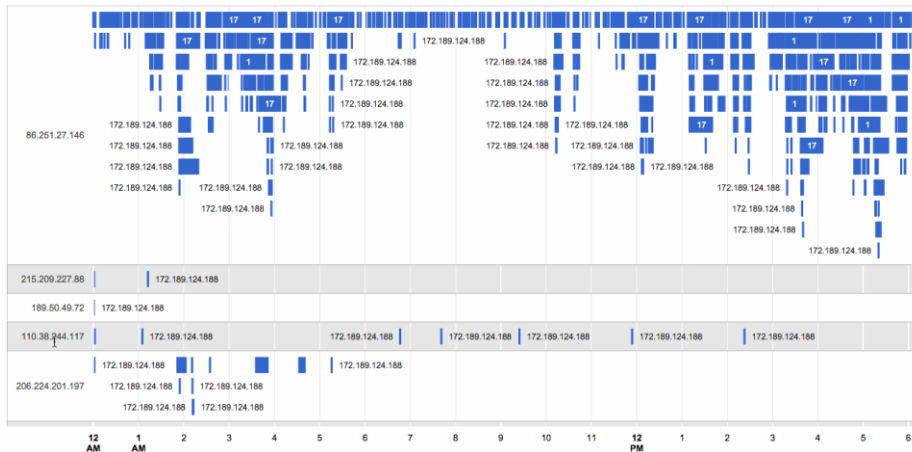
FlowPlotter - BubbleChart

- rwfilter ../Sampledata/sample.rw --type=all --proto=0-255 --pass=stdout | ./flowplotter.sh bubblechart sip > bubblechart.html



FlowPlotter - Timeline

- `rwfilter --proto=0- --type=out --sport=41142 --pass=stdout | ./flowplotter.sh timeline dip sip > timeline.html`

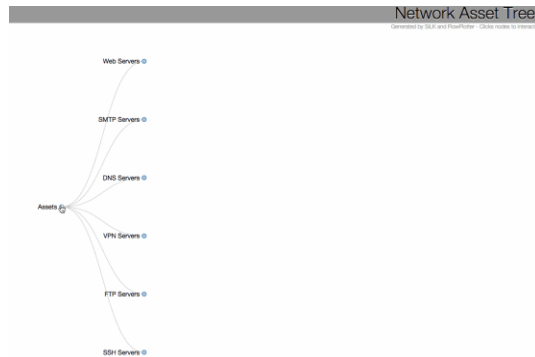


FlowPlotter - Force Directed

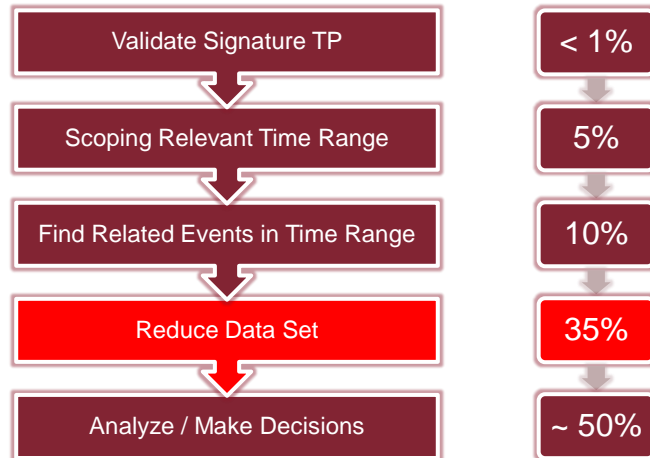
- `rwfilter ../Sampledata/sample.rw --scc=kr --proto=0- --type=all --pass=stdout | ./flowplotter.sh forcecapacity sip dip distinct:dport 100 > forcetest.html`

FlowPlotter - AssetDiscovery

- `rwfilter ../Sampledata/sample.rw --proto=0- --type=all --pass=stdout | ./flowplotter.sh assetdiscovery > assettest.html`



Flow in Analysis – PCAP Only

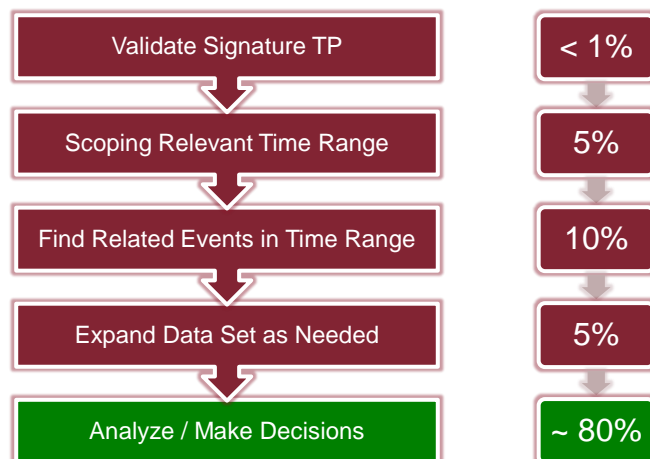


* Based on the First Hour of Analysis

MIRcon.
2014

45

Flow in Analysis - Improved



* Based on the First Hour of Analysis

MIRcon.
2014

46

Flow – Barriers to Entry

- Be Prepared to Look at a LOT of Line-Based Data
- Very Command Line Oriented
- Not Welcoming to Junior-Level Analysts
- Hard to Display/Interpret Data Visually

SiLK Data Output

```
smith@flowbat: ~ (ssh)
46.182.109.151 50.116.29.253 36861 22 6 12 1160 PS PA 2014/09/13T13:07:14.115 2.441 2014/09/13T13:07:16.556 50
46.182.109.151 50.116.29.253 37852 22 6 12 1160 PS PA 2014/09/13T13:07:16.525 2.374 2014/09/13T13:07:18.899 50
46.182.109.151 50.116.29.253 37242 22 6 12 1152 PS PA 2014/09/13T13:07:18.869 2.121 2014/09/13T13:07:40.990 50
46.182.109.151 50.116.29.253 37417 22 6 12 1160 PS PA 2014/09/13T13:07:40.959 2.072 2014/09/13T13:07:43.031 50
46.182.109.151 50.116.29.253 37603 22 6 12 1152 PS PA 2014/09/13T13:07:42.999 2.071 2014/09/13T13:07:45.070 50
50.116.29.253 46.182.109.151 22 55897 6 14 2601 PS PA 2014/09/13T13:00:36.655 2.386 2014/09/13T13:00:39.041 50
50.116.29.253 46.182.109.151 22 55266 6 14 2601 PS PA 2014/09/13T13:00:39.011 2.466 2014/09/13T13:00:41.477 50
50.116.29.253 46.182.109.151 22 55446 6 14 2601 PS PA 2014/09/13T13:00:41.445 1.737 2014/09/13T13:00:43.102 50
50.116.29.253 46.182.109.151 22 55590 6 14 2601 PS PA 2014/09/13T13:00:43.151 2.341 2014/09/13T13:00:45.432 50
50.116.29.253 46.182.109.151 22 55769 6 14 2601 PS PA 2014/09/13T13:00:45.461 2.952 2014/09/13T13:00:48.413 50
50.116.29.253 46.182.109.151 22 55959 6 14 2601 PS PA 2014/09/13T13:00:48.382 2.024 2014/09/13T13:00:50.406 50
50.116.29.253 46.182.109.151 22 56138 6 14 2601 PS PA 2014/09/13T13:00:50.376 2.631 2014/09/13T13:00:53.409 50
50.116.29.253 46.182.109.151 22 56292 6 14 2601 PS PA 2014/09/13T13:00:52.978 1.715 2014/09/13T13:00:54.693 50
50.116.29.253 46.182.109.151 22 56402 6 14 2601 PS PA 2014/09/13T13:00:54.662 2.184 2014/09/13T13:00:56.946 50
50.116.29.253 46.182.109.151 22 56573 6 14 2601 PS PA 2014/09/13T13:00:56.816 2.934 2014/09/13T13:00:59.750 50
50.116.29.253 46.182.109.151 22 56771 6 14 2601 PS PA 2014/09/13T13:00:59.720 2.006 2014/09/13T13:01:01.726 50
50.116.29.253 46.182.109.151 22 56930 6 14 2601 PS PA 2014/09/13T13:01:01.695 2.400 2014/09/13T13:01:04.583 50
50.116.29.253 46.182.109.151 22 57124 6 14 2601 PS PA 2014/09/13T13:01:04.152 2.228 2014/09/13T13:01:06.380 50
50.116.29.253 46.182.109.151 22 57300 6 14 2601 PS PA 2014/09/13T13:01:06.349 2.583 2014/09/13T13:01:08.852 50
50.116.29.253 46.182.109.151 22 57481 6 14 2601 PS PA 2014/09/13T13:01:08.821 2.914 2014/09/13T13:01:11.735 50
50.116.29.253 46.182.109.151 22 57678 6 14 2601 PS PA 2014/09/13T13:01:11.782 1.996 2014/09/13T13:01:13.698 50
50.116.29.253 46.182.109.151 22 57849 6 14 2601 PS PA 2014/09/13T13:01:13.667 2.466 2014/09/13T13:01:16.133 50
50.116.29.253 46.182.109.151 22 58031 6 14 2601 PS PA 2014/09/13T13:01:16.101 2.205 2014/09/13T13:01:18.306 50
50.116.29.253 46.182.109.151 22 58226 6 14 2601 PS PA 2014/09/13T13:01:18.275 2.494 2014/09/13T13:01:20.769 50
50.116.29.253 46.182.109.151 22 58400 6 14 2601 PS PA 2014/09/13T13:01:20.737 2.897 2014/09/13T13:01:23.634 50
50.116.29.253 46.182.109.151 22 58596 6 14 2601 PS PA 2014/09/13T13:01:23.603 1.842 2014/09/13T13:01:25.446 50
50.116.29.253 46.182.109.151 22 58761 6 14 2601 PS PA 2014/09/13T13:01:25.415 2.445 2014/09/13T13:01:27.860 50
50.116.29.253 46.182.109.151 22 58943 6 14 2601 PS PA 2014/09/13T13:01:27.829 2.521 2014/09/13T13:01:30.350 50
50.116.29.253 46.182.109.151 22 59051 6 14 2601 PS PA 2014/09/13T13:01:30.320 2.466 2014/09/13T13:01:32.786 50
50.116.29.253 46.182.109.151 22 59110 6 14 2601 PS PA 2014/09/13T13:01:32.755 2.548 2014/09/13T13:01:35.303 50
50.116.29.253 46.182.109.151 22 59496 6 14 2601 PS PA 2014/09/13T13:01:35.272 1.813 2014/09/13T13:01:37.085 50
50.116.29.253 46.182.109.151 22 59632 6 14 2601 PS PA 2014/09/13T13:01:37.064 2.431 2014/09/13T13:01:39.485 50
50.116.29.253 46.182.109.151 22 59839 6 14 2601 PS PA 2014/09/13T13:01:39.453 3.036 2014/09/13T13:01:42.489 50
50.116.29.253 46.182.109.151 22 60005 6 14 2601 PS PA 2014/09/13T13:01:42.458 2.111 2014/09/13T13:01:44.569 50
50.116.29.253 46.182.109.151 22 60232 6 14 2601 PS PA 2014/09/13T13:01:44.539 2.731 2014/09/13T13:01:47.254 50
50.116.29.253 46.182.109.151 22 60415 6 14 2601 PS PA 2014/09/13T13:01:47.224 1.805 2014/09/13T13:01:49.029 50
50.116.29.253 46.182.109.151 22 60576 6 14 2601 PS PA 2014/09/13T13:01:48.997 2.486 2014/09/13T13:01:51.405 50
50.116.29.253 46.182.109.151 22 60736 6 14 2601 PS PA 2014/09/13T13:01:51.372 3.013 2014/09/13T13:01:54.385 50
50.116.29.253 46.182.109.151 22 60913 6 14 2601 PS PA 2014/09/13T13:01:54.354 2.089 2014/09/13T13:01:56.443 50
50.116.29.253 46.182.109.151 22 61066 6 14 2601 PS PA 2014/09/13T13:01:56.413 2.781 2014/09/13T13:01:59.116 50
50.116.29.253 46.182.109.151 22 61302 6 14 2601 PS PA 2014/09/13T13:01:59.886 1.775 2014/09/13T13:02:00.861 50
50.116.29.253 46.182.109.151 22 61375 6 14 2601 PS PA 2014/09/13T13:02:00.829 2.386 2014/09/13T13:02:03.233 50
50.116.29.253 46.182.109.151 22 61546 6 14 2601 PS PA 2014/09/13T13:02:03.195 3.450 2014/09/13T13:02:06.193 50
50.116.29.253 46.182.109.151 22 61552 6 14 2601 PS PA 2014/09/13T13:02:06.163 2.076 2014/09/13T13:02:08.239 50
50.116.29.253 46.182.109.151 22 61721 6 14 2601 PS PA 2014/09/13T13:02:08.200 2.084 2014/09/13T13:02:10.892 50
50.116.29.253 46.182.109.151 22 61910 6 14 2601 PS PA 2014/09/13T13:02:10.861 2.182 2014/09/13T13:02:12.963 50
50.116.29.253 46.182.109.151 22 62068 6 14 2601 PS PA 2014/09/13T13:02:12.931 2.363 2014/09/13T13:02:15.294 50
50.116.29.253 46.182.109.151 22 62352 6 14 2601 PS PA 2014/09/13T13:02:15.264 3.044 2014/09/13T13:02:18.308 50
50.116.29.253 78.47.206.247 22 64200 6 14 4340 PS PA 2014/09/13T13:02:18.684 5.466 2014/09/13T13:02:19.350 50
50.116.29.253 46.182.109.151 22 64456 6 14 2601 PS PA 2014/09/13T13:02:18.277 2.070 2014/09/13T13:02:20.347 50
```


FLOWBAT

Q Execute each 5 minutes - Command line Query builder Records Stats Count

UTC: 2014/09/11 13:11

rwfilter --sensor=50 --type=all --sport=80

Exclusions --daddress=192.168.0.1 OR --scc=au

Source IP	Destination IP	Source port	Destination port	IP protocol	Packet count	Byte count	TCP flags	Starting time	Duration	End time	Sensor
50.116.29.253	192.99.39.78	80	44926	6	1	40	RA	2014/09/11 01:54:38.796	0.000	2014/09/11 01:54:38.796	50
50.116.29.253	192.99.201.184	80	19887	6	1	40	RA	2014/09/11 02:37:20.783	0.000	2014/09/11 02:37:20.783	50
50.116.29.253	54.87.87.26	80	51779	6	1	40	RA	2014/09/11 02:45:28.924	0.000	2014/09/11 02:45:28.924	50
50.116.29.253	218.77.79.43	80	41885	6	1	40	RA	2014/09/11 03:27:39.256	0.000	2014/09/11 03:27:39.256	50
50.116.29.253	107.22.2.97	80	56051	6	1	40	RA	2014/09/11 03:41:00.749	0.000	2014/09/11 03:41:00.749	50
92.222.167.198	50.116.29.253	80	4198	6	1	44	SA	2014/09/11 04:01:13.618	0.000	2014/09/11 04:01:13.618	50
50.116.29.253	222.35.16.27	80	58898	6	1	40	RA	2014/09/11 05:04:55.057	0.000	2014/09/11 05:04:55.057	50
23.20.48.204	50.116.29.253	80	55142	6	5	404	FSPA	2014/09/11 06:37:42.964	0.068	2014/09/11 06:37:43.032	50
23.20.48.204	50.116.29.253	80	55143	6	5	404	FSPA	2014/09/11 06:37:43.231	0.094	2014/09/11 06:37:43.325	50
23.20.48.204	50.116.29.253	80	55144	6	5	405	FSPA	2014/09/11 06:37:43.325	0.067	2014/09/11 06:37:43.392	50

MIRcon 2014 49

FLOWBAT

- Flow Basic Analysis Tool
- Graphical Front-End to SiLK
- Easy Two-Step Install on SiLK Capable Box
 - Install Locally to SiLK Box
 - Install Remotely and Interact via SSH w/ Keys
- Rapid Pivoting Between Data
- Graphing Ability
- By Analysts, for Analysts

MIRcon 2014 50

Getting Data with FlowBAT (CLI Mode)

FLOWBAT Dashboard Quick Query Saved Queries IP Sets Chris Sanders ▾

Q Execute ▾ Command line Query builder UTC: 2014/09/29 17:00

rwfilter ⓘ

Exclusions Use "OR" to separate exclusions, for example: --type=7 OR --dport=80

Output type

Records Stats Count

MIRcon. 2014 51

Getting Data with FlowBAT (Guided Mode)

FLOWBAT Dashboard Quick Query Saved Queries IP Sets Chris Sanders ▾

Q Execute ▾ Command line Query builder UTC: 2014/09/29 17:01

Input options

Start date (switch to offset) End date

yyyy/mm/dd yyyy/mm/dd

Types Sensor

Select Some Options

Partitioning options

Source IP Source port

Destination IP Destination port

Any IP Any port

Protocol Flags

MIRcon. 2014 52

Manipulating FlowBAT Data

Exclusions Use "OR" to separate exclusions, for example: --type=7 OR --dport=80

Output type

Records Stats Count

Starting time	Source IP	Destination IP	Source port	Destination port	IP protocol	Packet count	Byte count	TCP flags	Duration	End time	Sensor
2014/09/29 05:00:49.856	162.212.181.242	50.116.29.253	60615	53	17	1	84		0.000	2014/09/29 05:00:49.856	50
2014/09/29 05:39:05.133	162.212.181.242	50.116.29.253	17230	53	17	1	84		0.000	2014/09/29 05:39:05.133	50
2014/09/29 05:51:49.380	162.212.181.242	50.116.29.253	28970	53	17	1	84		0.000	2014/09/29 05:51:49.380	50
2014/09/29 06:30:03.388	162.212.181.242	50.116.29.253	60416	53	17	1	84		0.000	2014/09/29 06:30:03.388	50
2014/09/29 07:08:15.617	162.212.181.242	50.116.29.253	7348	53	17	1	84		0.000	2014/09/29 07:08:15.617	50
2014/09/29 10:06:26.139	162.212.181.242	50.116.29.253	41846	53	17	1	84		0.000	2014/09/29 10:06:26.139	50
2014/09/29 11:10:06.287	162.212.181.242	50.116.29.253	60578	53	17	1	84		0.000	2014/09/29 11:10:06.287	50
2014/09/29 12:01:01.156	162.212.181.242	50.116.29.253	21537	53	17	1	84		0.000	2014/09/29 12:01:01.156	50
2014/09/29 14:33:40.225	162.212.181.242	50.116.29.253	38104	53	17	1	84		0.000	2014/09/29 14:33:40.225	50
2014/09/29 16:15:26.648	162.212.181.242	50.116.29.253	58226	53	17	1	84		0.000	2014/09/29 16:15:26.648	50

< Previous 10 per page Next >

Pivoting with FlowBAT Data

Execute Command line Query builder UTC: 2014/09/29 17:18

rwfilter --type=all --dport=53 --any-address=162.212.181.0/24

Exclusions Use "OR" to separate exclusions, for example: --type=7 OR --dport=80

Output type

Records Stats Count

Starting time	End time	Source IP	Destination IP	Source port	Destination port	Packet count	Byte count	TCP flags	Duration	Sensor
2014/09/29 05:00:49.856	2014/09/29 05:00:49.856	162.212.181.242	50.116.29.253	60615	53	1	84		0.000	50
2014/09/29 05:39:05.133	2014/09/29 05:39:05.133	162.212.181.242	50.116.29.253	17230	53	1	84		0.000	50
2014/09/29 05:51:49.380	2014/09/29 05:51:49.380	162.212.181.242	50.116.29.253	28970	53	1	84		0.000	50
2014/09/29 06:30:03.388	2014/09/29 06:30:03.388	162.212.181.242	50.116.29.253	60416	53	1	84		0.000	50
2014/09/29 07:08:15.617	2014/09/29 07:08:15.617	162.212.181.242	50.116.29.253	7348	53	1	84		0.000	50
2014/09/29 10:06:26.139	2014/09/29 10:06:26.139	162.212.181.242	50.116.29.253	41846	53	1	84		0.000	50
2014/09/29 11:10:06.287	2014/09/29 11:10:06.287	162.212.181.242	50.116.29.253	60578	53	1	84		0.000	50
2014/09/29 12:01:01.156	2014/09/29 12:01:01.156	162.212.181.242	50.116.29.253	21537	53	1	84		0.000	50
2014/09/29 14:33:40.225	2014/09/29 14:33:40.225	162.212.181.242	50.116.29.253	38104	53	1	84		0.000	50
2014/09/29 16:15:26.648	2014/09/29 16:15:26.648	162.212.181.242	50.116.29.253	58226	53	1	84		0.000	50

Generating Stats with FlowBAT

Final query

```
$ rfilter --type=all --start-date=2014/09/29:21 --active-time=2014/09/29T21:35:14.003-2014/09/29T22:35:14.003 --dport=1825- --sport=1825- --protocol=0-255 --pass=stdout > /tmp/AD2CYK2AZfax7bvbz.rwf  
$ rwstats --delimited --fields=sIP,dIP --values=Bytes --top --count=10 /tmp/AD2CYK2AZfax7bvbz.rwf
```

Q Execute Command line Query builder

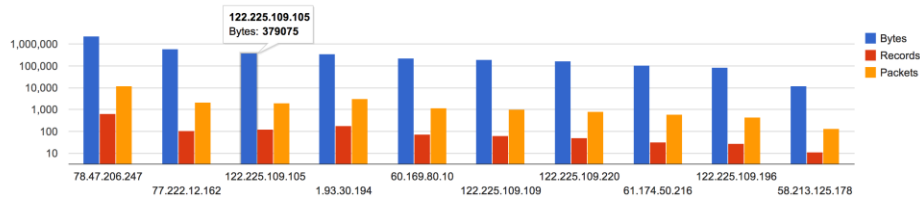
Source IP	Destination IP	Bytes	% Bytes	% Cumulative
198.143.173.180	50.116.29.253	426	46.968026	46.968026
201.186.63.136	50.116.29.253	156	17.199559	64.167585
50.116.29.253	201.186.63.136	120	13.230430	77.398015
198.20.70.114	50.116.29.253	45	4.961411	82.359427
116.255.204.235	50.116.29.253	40	4.410143	86.769570
50.116.29.253	116.255.204.235	40	4.410143	91.179713
219.140.170.70	50.116.29.253	40	4.410143	95.589857
50.116.29.253	219.140.170.70	40	4.410143	100.000000

Generating Stats with FlowBAT

Final query

```
$ rfilter --type=in --dport=22 --packets=4- --ack-flag=1 --pass=stdout | rfilter --input-pipe=stdin --sccc-- --fail=stdout > /tmp/szoY2QPne3TsXk5q.rwf  
$ rwstats --delimited --fields=sIP --values=Bytes,Records,Packets --top --count=10 /tmp/szoY2QPne3TsXk5q.rwf
```

Q Execute each 60 minutes Command line Query builder



Conclusion

- Flow Data is Underused and Underrated
- Easy to Collect, Enhances Detection & Analysis
- Minimal Barriers to Entry
 - SiLK (Easy to Install on SO)
 - Argus (Already Installed on SO)
 - Bro (Already Installed on SO)

Thanks Folks!

- Questions?
 - Chris Sanders – chris@chrissanders.org
 - Jason Smith – jason.smith.webmail@gmail.com
- Blog / Book
 - <http://www.appliednsm.com>
- FlowPlotter
 - <http://www.github.com/automayt/FlowPlotter/>
- FlowBAT
 - <http://www.flowbat.com>