Real-Time Visualization of Network Behaviors for Situational Awareness

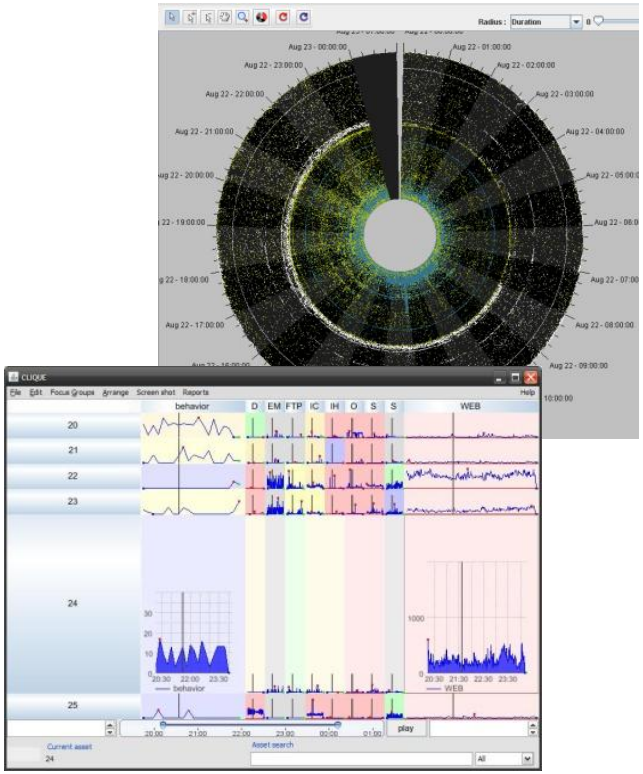
Daniel Best {daniel.best@pnl.gov}
Pacific Northwest National Laboratory

Shawn Bohn, Douglas Love, Adam Wynne, William Pike

Challenges to overcome

- Thousands of flow records per second
  - More network flow data than a human can possibly review
- Real-time availability
  - Knowing what is happening as it's happening
- Making sense of it all
  - What is normal, is this activity expected?

Our contributions

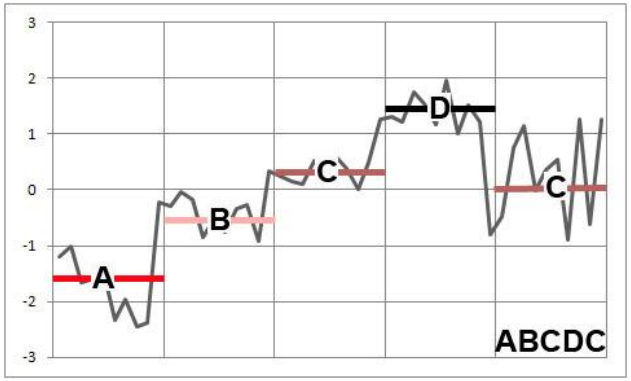


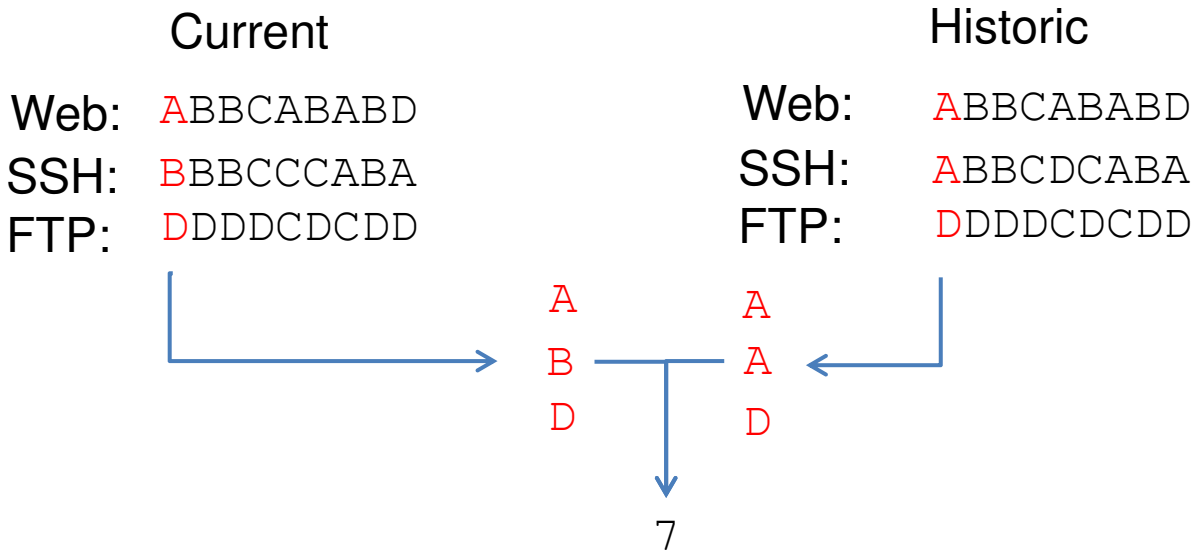
- Traffic Circle
  - Visualization for situational awareness
- Correlation Layers for Information Query and Exploration (CLIQUE)
  - Network behavior visualization using LiveRac interface
- Middleware for Data-Intensive Computing (MeDiCi)
  - Data pipeline

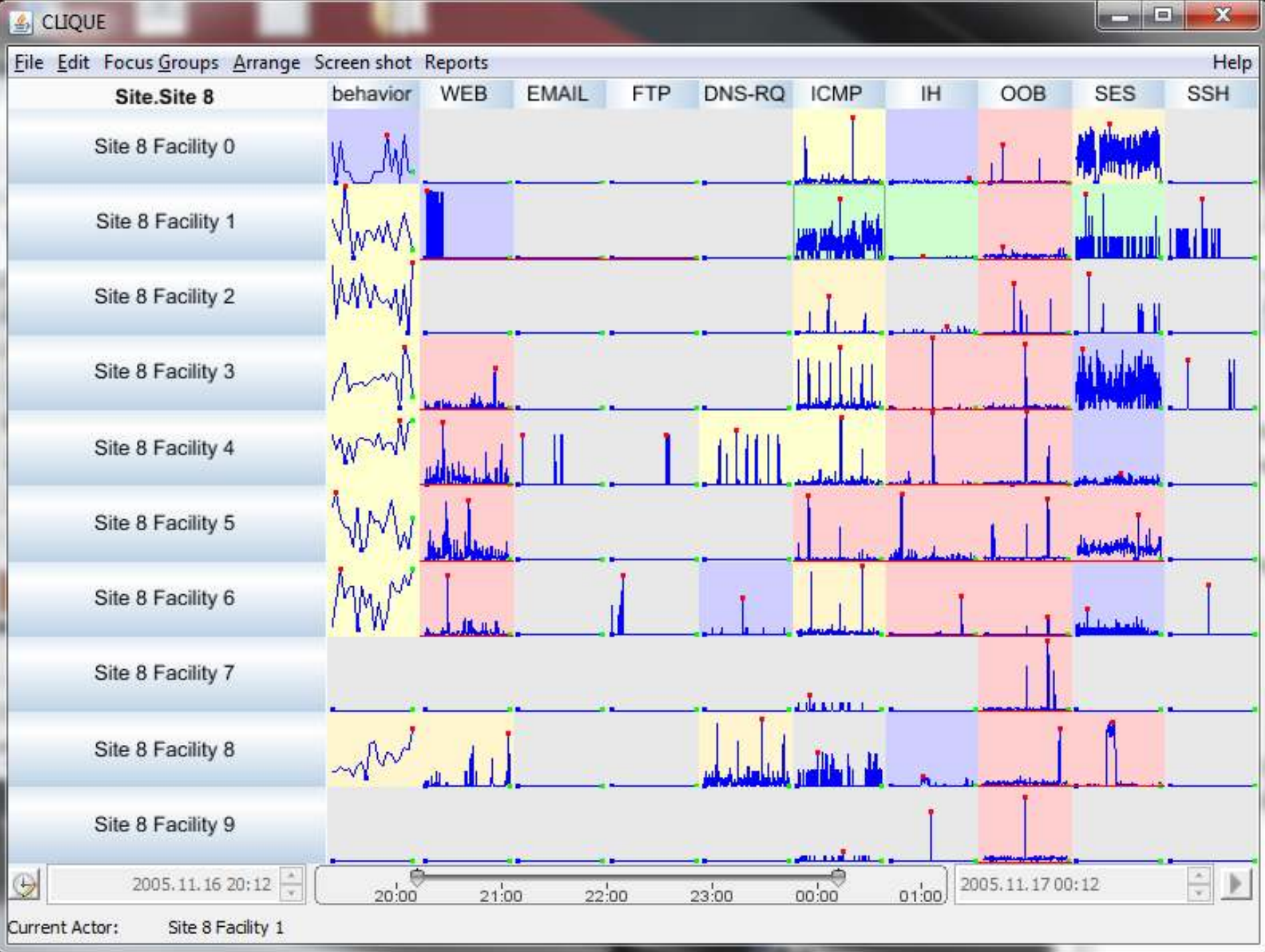
CLIQUE: Find a starting point

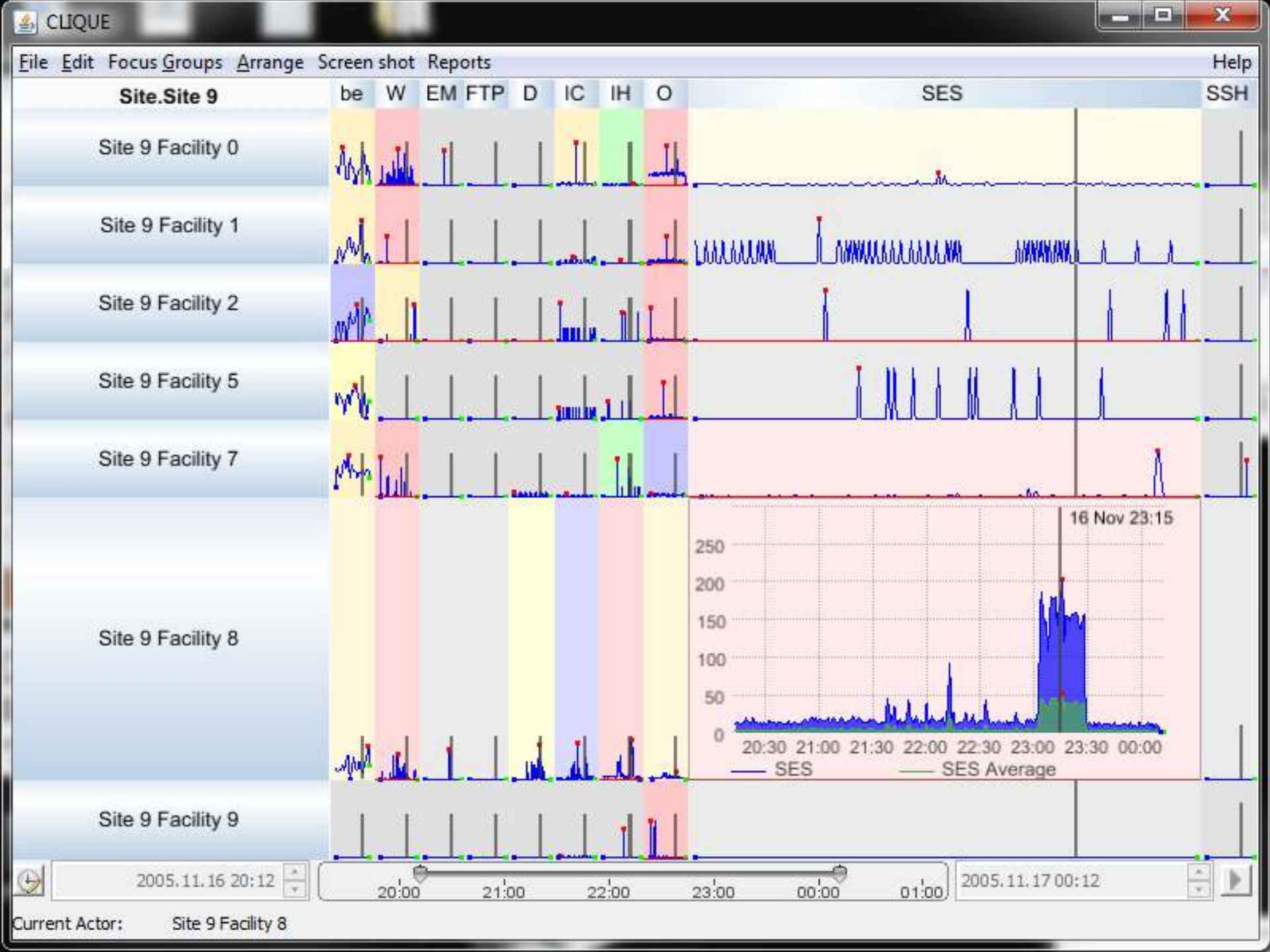
- Behavior baseline for actors
  - Creates statistical model of what is normal for a given actor and category set
  - Visualizes the distance from normal activity
- Arbitrary actor hierarchy
  - Groups of IP addresses or just a single IP address
  - Analyst independent, can be shared
- Interactive interface which highlights thresholds and provides semantic zooming

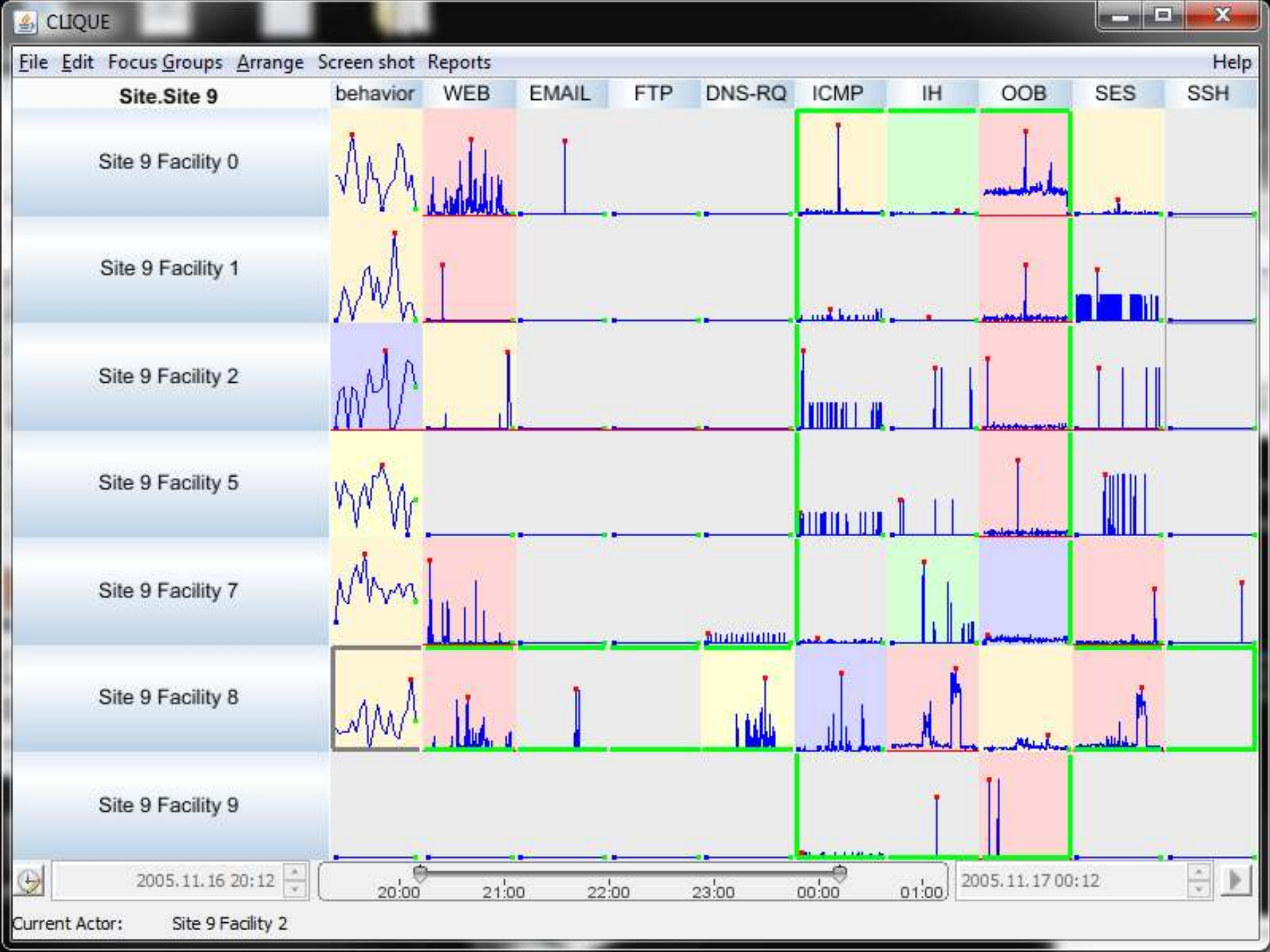
CLIQUE: Behavior





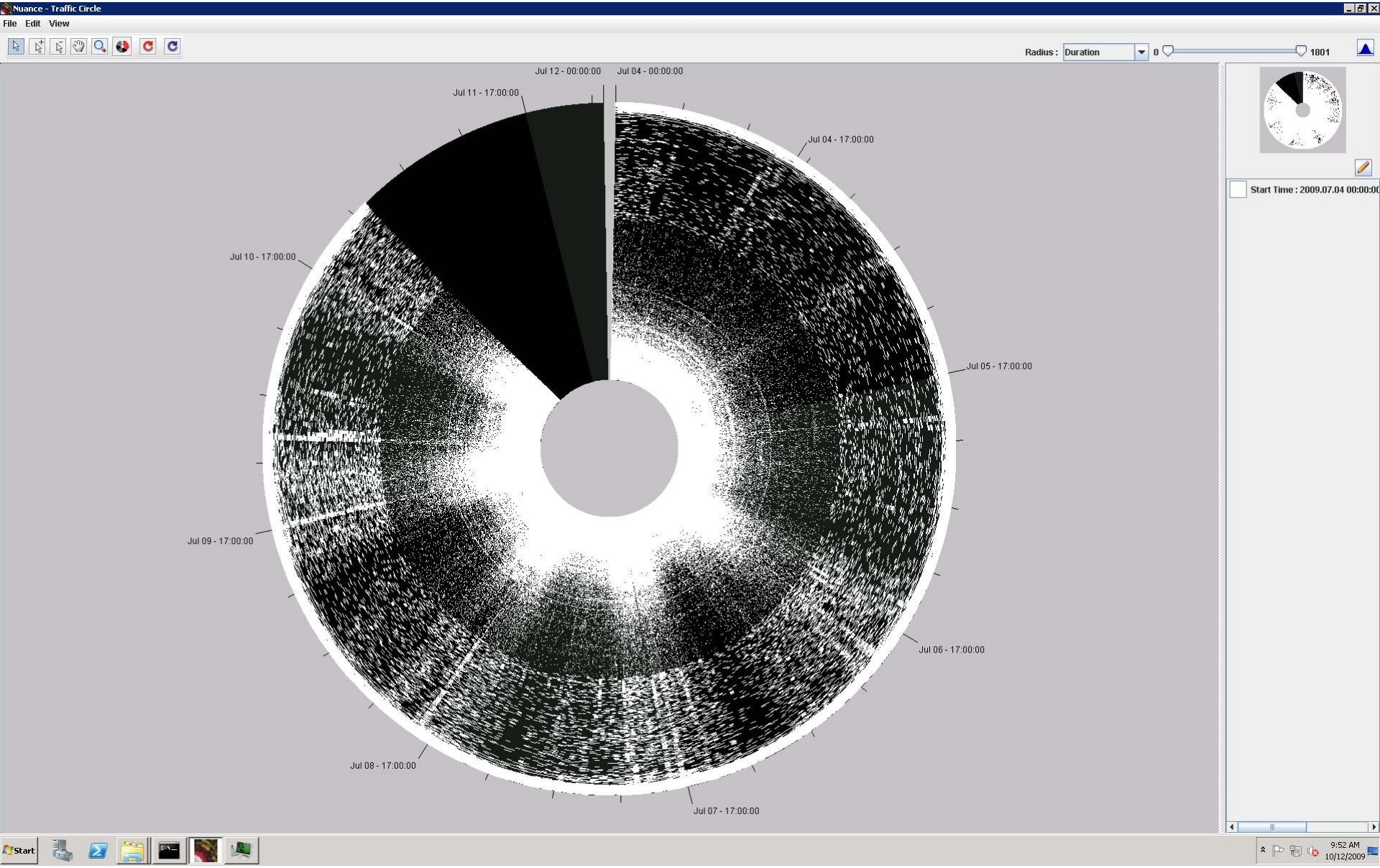

CLIQUE
File Edit Focus Groups Arrange Screen shot Reports Help
Site.Site 8
behavior
WEB
EMAIL
FTP
DNS-RQ
ICMP
IH
OOB
SES
SSH
Site 8 Facility 0
Site 8 Facility 1
Site 8 Facility 2
Site 8 Facility 3
Site 8 Facility 4
Site 8 Facility 5
Site 8 Facility 6
Site 8 Facility 7
Site 8 Facility 8
Site 8 Facility 9
2005.11.16 20:12
20:00
21:00
22:00
23:00
00:00
01:00
2005.11.17 00:12
Current Actor: Site 8 Facility 1

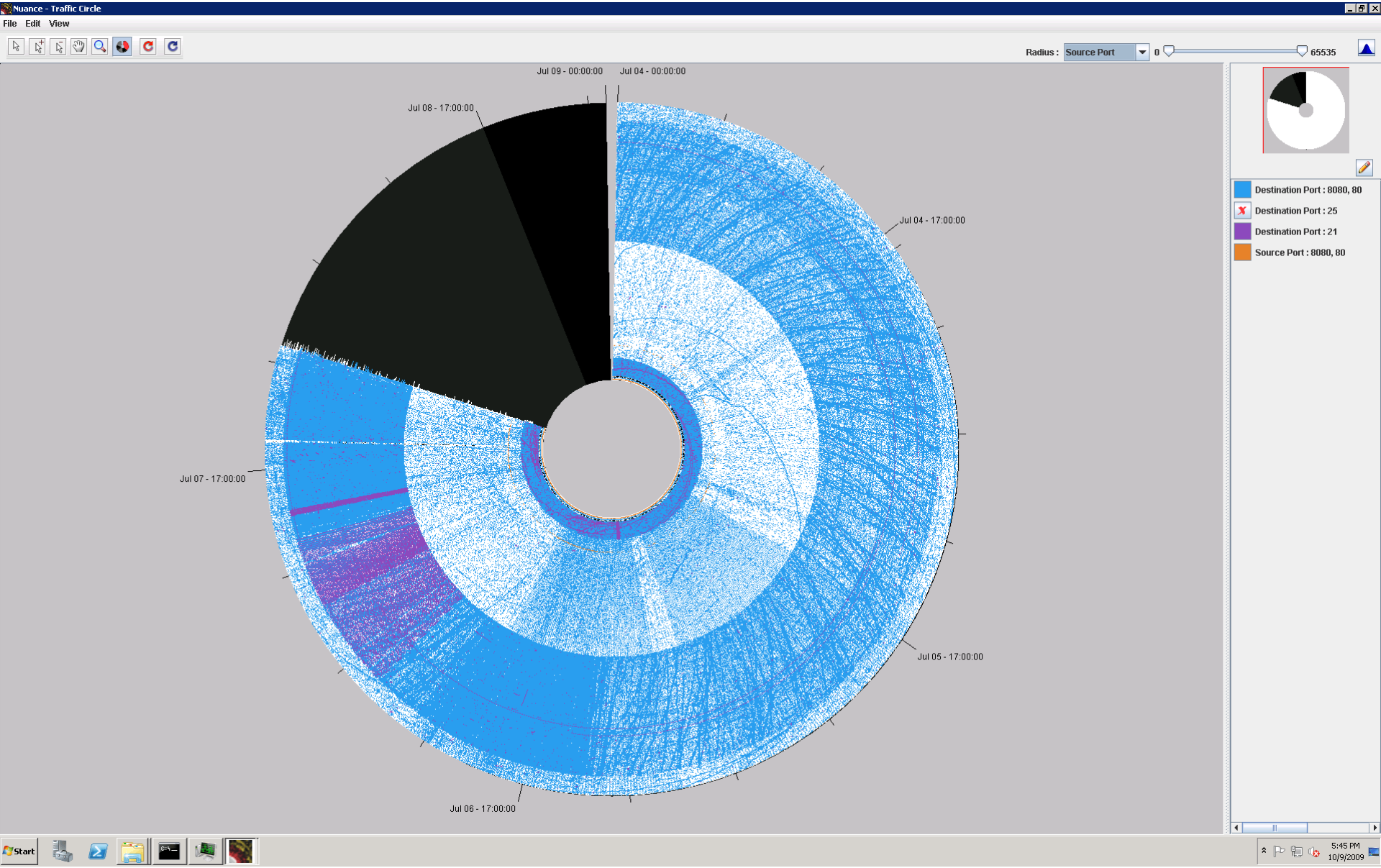

CLIQUE
File Edit Focus Groups Arrange Screen shot Reports Help
Site.Site 9
be W EM FTP D IC IH O
SES
SSH
Site 9 Facility 0
Site 9 Facility 1
Site 9 Facility 2
Site 9 Facility 5
Site 9 Facility 7
Site 9 Facility 8
Site 9 Facility 9
16 Nov 23:15
250
200
150
100
50
0
20:30 21:00 21:30 22:00 22:30 23:00 23:30 00:00
SES
SES Average
2005.11.16 20:12
20:00 21:00 22:00 23:00 00:00 01:00
2005.11.17 00:12
Current Actor: Site 9 Facility 8

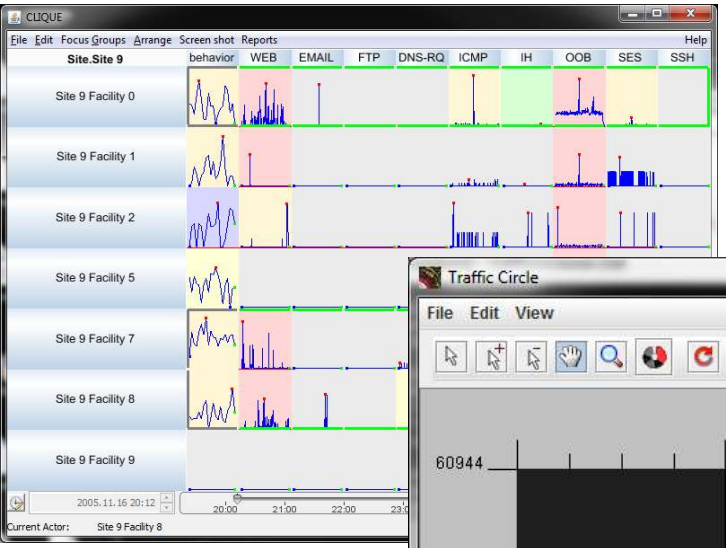

CLIQUE
File Edit Focus Groups Arrange Screen shot Reports Help
Site.Site 9
behavior
WEB
EMAIL
FTP
DNS-RQ
ICMP
IH
OOB
SES
SSH
Site 9 Facility 0
Site 9 Facility 1
Site 9 Facility 2
Site 9 Facility 5
Site 9 Facility 7
Site 9 Facility 8
Site 9 Facility 9
2005.11.16 20:12
20:00
21:00
22:00
23:00
00:00
01:00
2005.11.17 00:12
Current Actor: Site 9 Facility 2

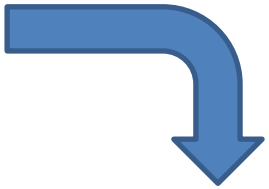
Traffic Circle: Find understanding

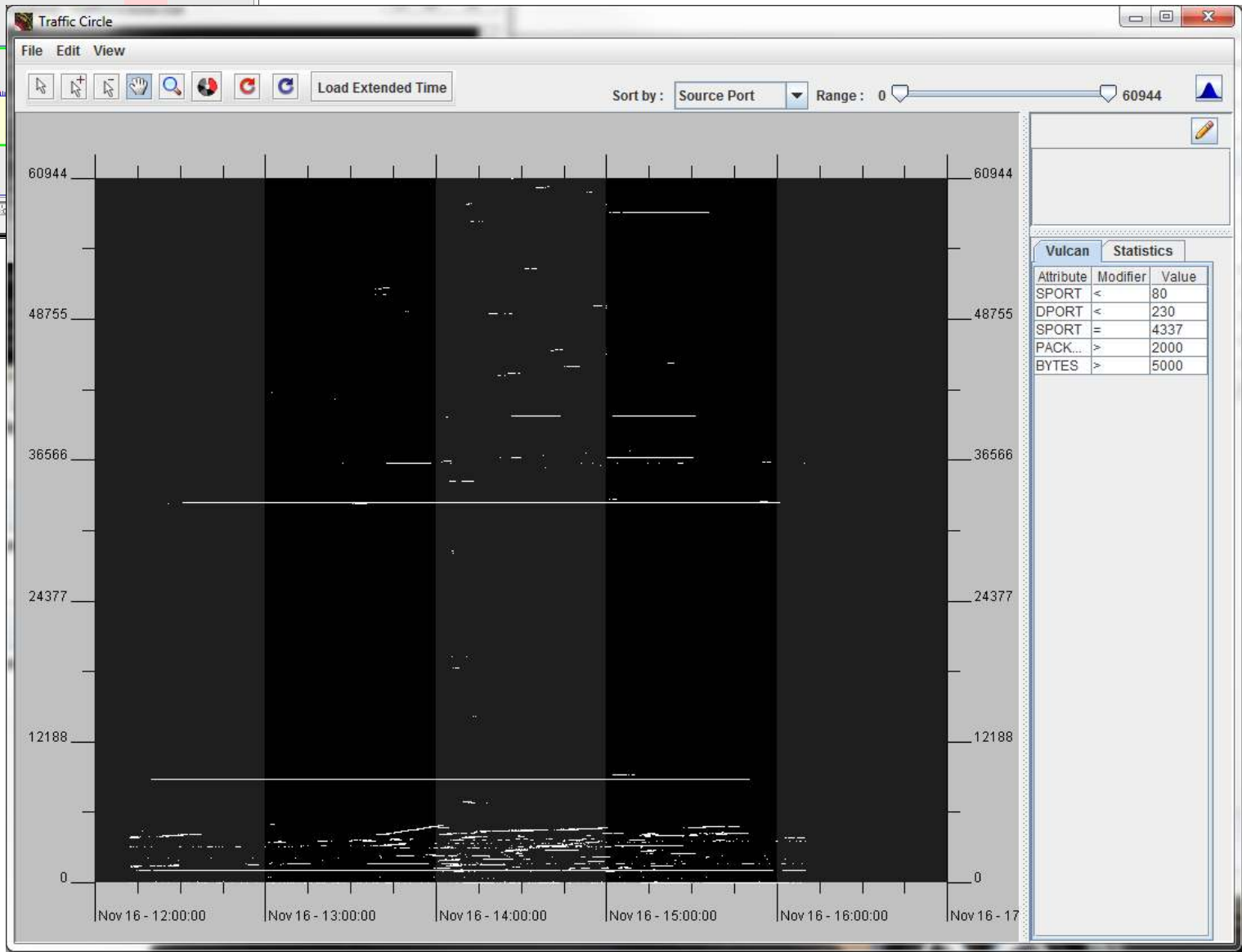
- Interactive and scalable flow plot visualization
  - Capable of visualizing 100 Million + flow records
  - Allows exploration of the dataspace and draws out features
  - The more memory and pixels, the more the tool can display
- Layer style filters
  - color encoding
  - data hiding
- While listening to incoming flow records, Traffic Circle will spin clockwise on a heartbeat

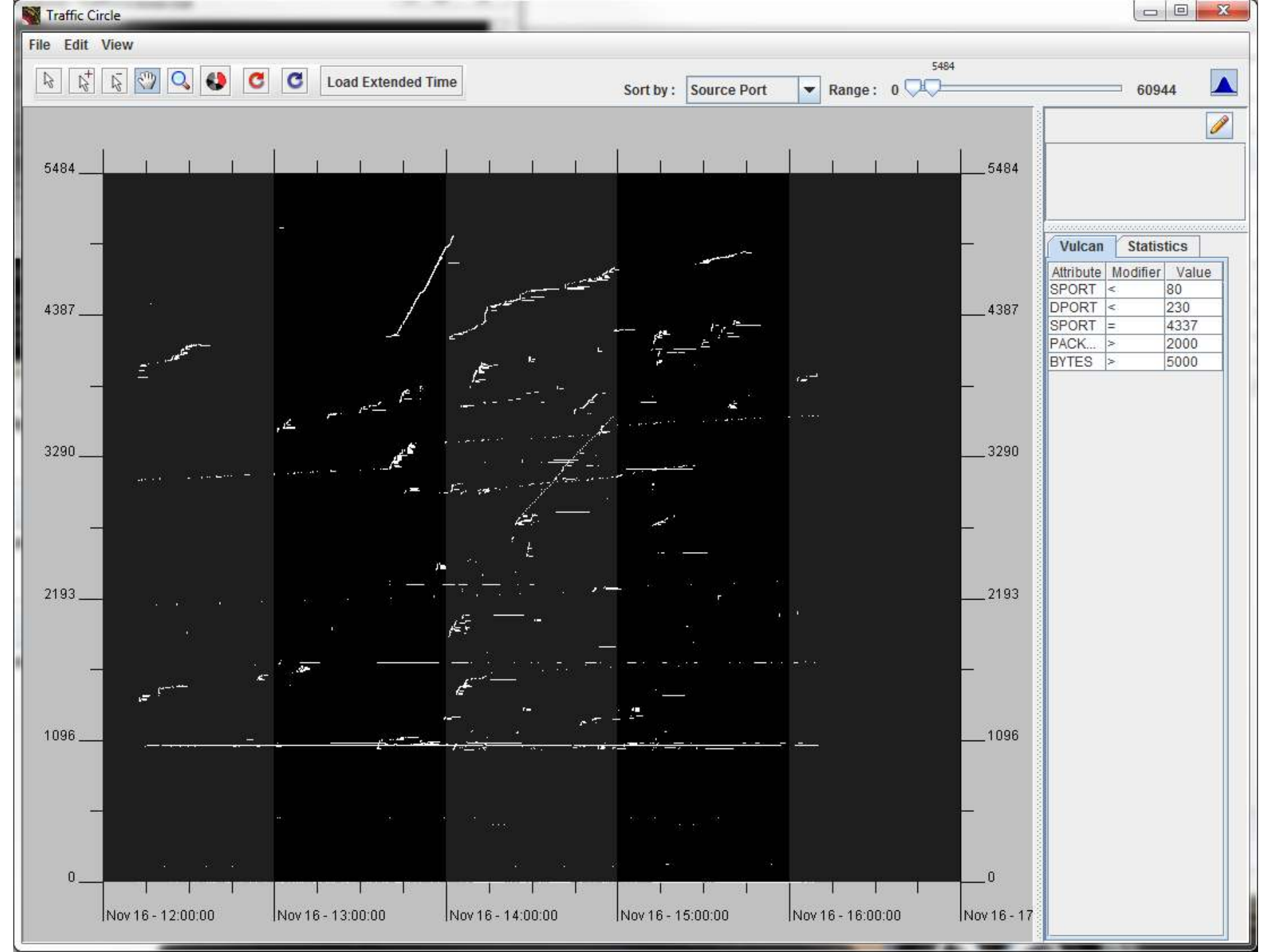

Nuance - Traffic Circle
File Edit View
Radius : Duration 0 1801
Jul 12 - 00:00:00
Jul 04 - 00:00:00
Jul 11 - 17:00:00
Jul 04 - 17:00:00
Jul 10 - 17:00:00
Jul 05 - 17:00:00
Jul 09 - 17:00:00
Jul 06 - 17:00:00
Jul 08 - 17:00:00
Jul 07 - 17:00:00
Start Time : 2009.07.04 00:00:00
Start
9:52 AM
10/12/2009

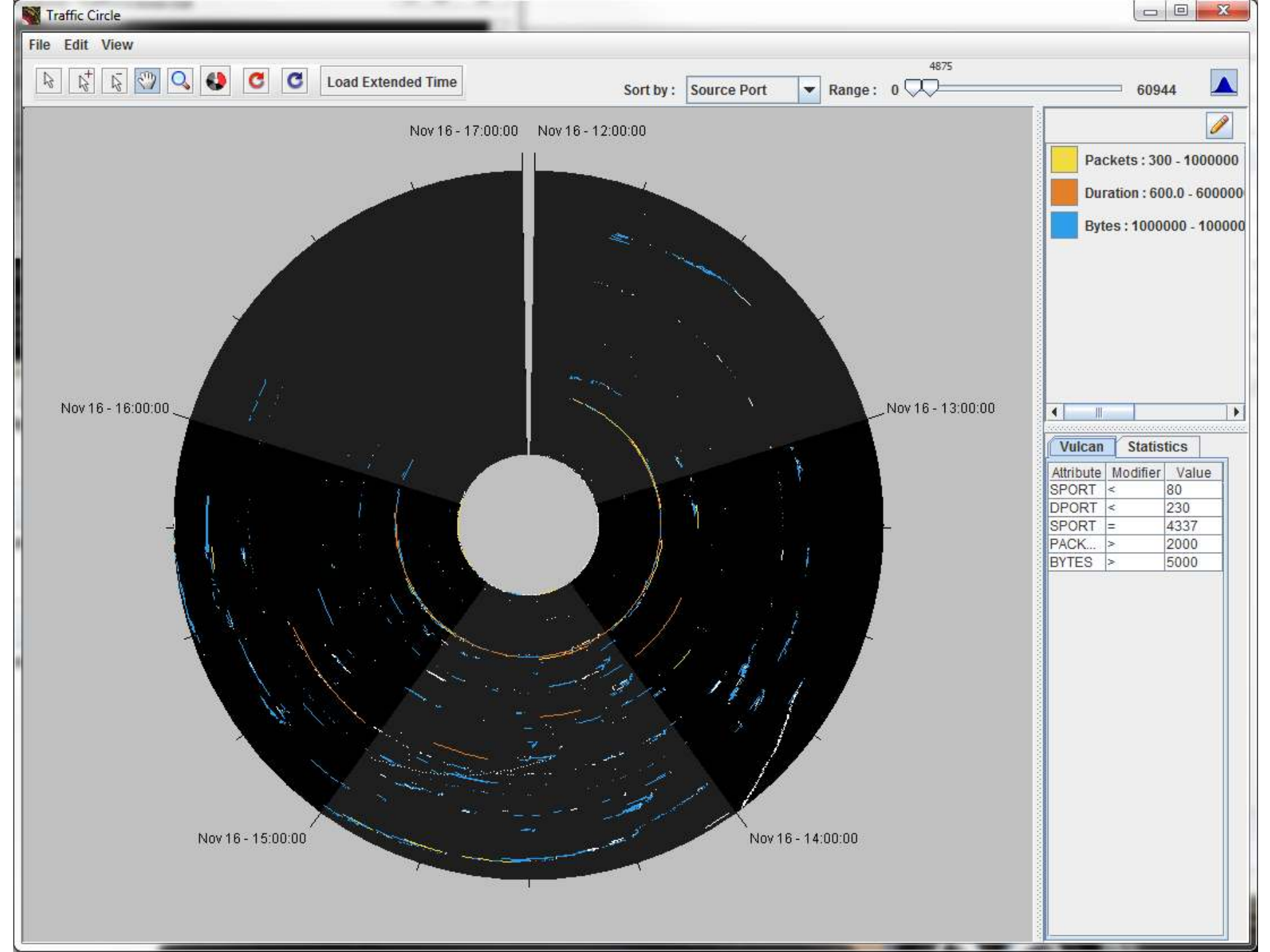

Nuance - Traffic Circle
File Edit View
Radius : Source Port 0 65535
Jul 09 - 00:00:00
Jul 04 - 00:00:00
Jul 08 - 17:00:00
Jul 04 - 17:00:00
Jul 07 - 17:00:00
Jul 05 - 17:00:00
Jul 06 - 17:00:00
Destination Port : 8080, 80
Destination Port : 25
Destination Port : 21
Source Port : 8080, 80
Start
5:45 PM
10/9/2009

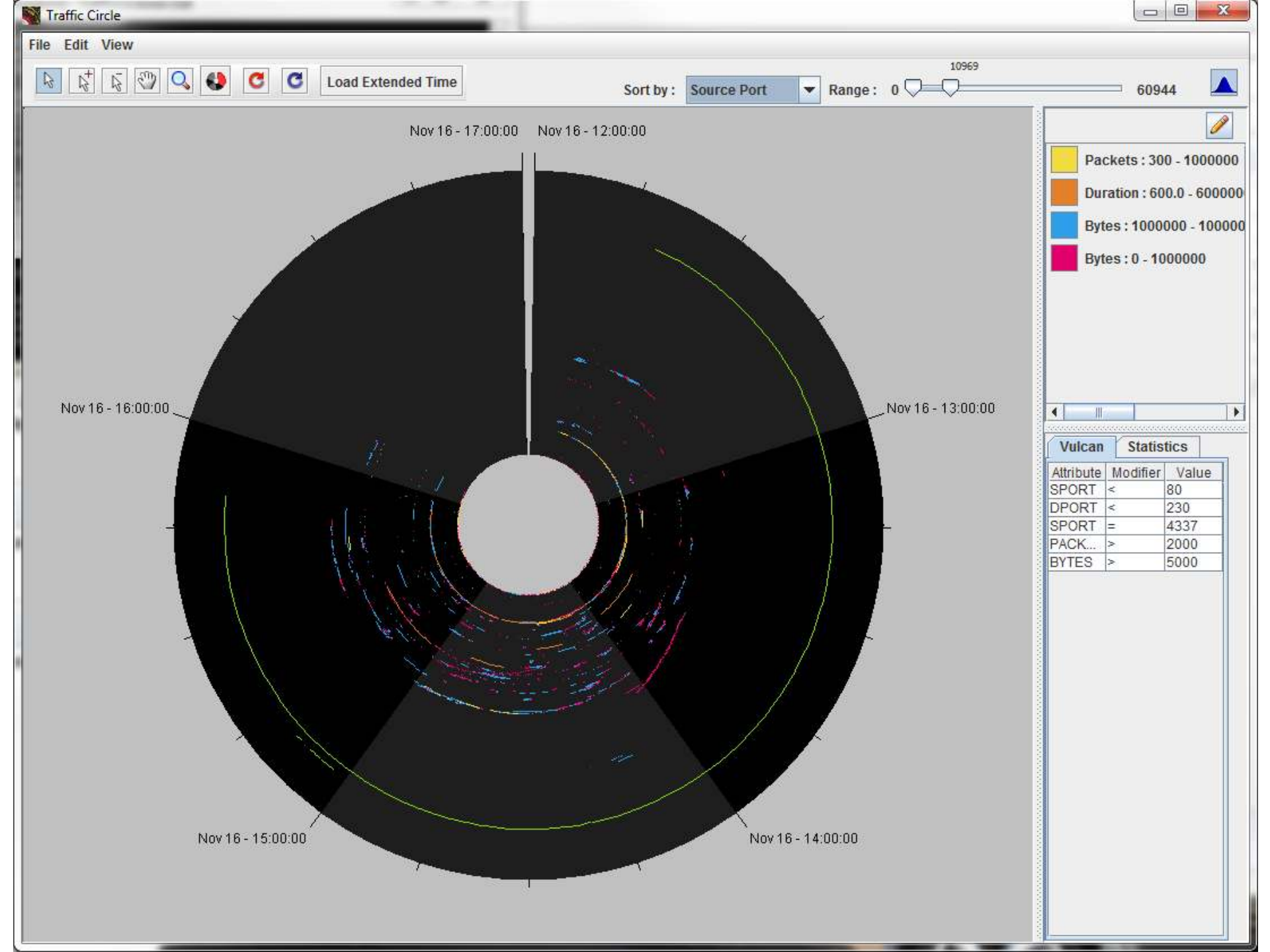

CLIQUE
File Edit Focus Groups Arrange Screen shot Reports Help
Site.Site 9
behavior WEB EMAIL FTP DNS-RQ ICMP IH OOB SES SSH
Site 9 Facility 0
Site 9 Facility 1
Site 9 Facility 2
Site 9 Facility 5
Site 9 Facility 7
Site 9 Facility 8
Site 9 Facility 9
2005.11.16 20:12
20:00 21:00 22:00
Current Actor: Site 9 Facility 8




Traffic Circle
File Edit View
Load Extended Time
Sort by : Source Port
Range : 0 60944
60944
48755
36566
24377
12188
0
Nov 16 - 12:00:00
Nov 16 - 13:00:00
Nov 16 - 14:00:00
Nov 16 - 15:00:00
Nov 16 - 16:00:00
Nov 16 - 17
Vulcan
Statistics
Attribute Modifier Value
SPORT < 80
DPORT < 230
SPORT = 4337
PACK... > 2000
BYTES > 5000


Traffic Circle
File Edit View
Load Extended Time
Sort by : Source Port
Range : 0 5484 60944
5484
4387
3290
2193
1096
0
Nov 16 - 12:00:00
Nov 16 - 13:00:00
Nov 16 - 14:00:00
Nov 16 - 15:00:00
Nov 16 - 16:00:00
Nov 16 - 17
Vulcan
Statistics
Attribute Modifier Value
SPORT < 80
DPORT < 230
SPORT = 4337
PACK... > 2000
BYTES > 5000


Traffic Circle
File
Edit
View
Load Extended Time
Sort by :
Source Port
Range :
0
4875
60944
Nov 16 - 17:00:00
Nov 16 - 12:00:00
Nov 16 - 16:00:00
Nov 16 - 13:00:00
Nov 16 - 15:00:00
Nov 16 - 14:00:00
Packets : 300 - 1000000
Duration : 600.0 - 600000
Bytes : 1000000 - 100000
Vulcan
Statistics
Attribute
Modifier
Value
SPORT
<
80
DPORT
<
230
SPORT
=
4337
PACK...
>
2000
BYTES
>
5000


Traffic Circle
File
Edit
View
Load Extended Time
Sort by :
Source Port
Range :
0
10969
60944
Nov 16 - 17:00:00
Nov 16 - 12:00:00
Nov 16 - 16:00:00
Nov 16 - 13:00:00
Nov 16 - 15:00:00
Nov 16 - 14:00:00
Packets : 300 - 1000000
Duration : 600.0 - 600000
Bytes : 1000000 - 100000
Bytes : 0 - 1000000
Vulcan
Statistics
Attribute
Modifier
Value
SPORT
<
80
DPORT
<
230
SPORT
=
4337
PACK...
>
2000
BYTES
>
5000

Traffic Circle

< DIP

FLOWS	SIP	DIP	SPORT	DPORT	SASN	DASN	PROTO	PACKET SUM	BYTE SUM ▲	TIME
1	1	140.221.227.2...	1	1			1	1	770	2005.11.15 1...
1	1	140.221.201.2...	1	1			1	1	920	2005.11.14 1...
1	1	140.221.238.0...	1	1			1	2	1240	2005.11.15 1...
1	1	140.221.248.0...	1	1			1	2	1240	2005.11.14 1...
1	1	071.096.167.2...	1	1			1	3	2100	2005.11.15 1...
1	1	140.221.231.0...	1	1			1	2	2280	2005.11.14 1...
4	4	140.221.227.0...	4	1			1	5	3800	2005.11.14 1...
1	1	140.221.255.2...	1	1			1	1	4360	2005.11.15 1...
1	1	195.127.224.1...	1	1			1	2	8954	2005.11.16 1...
1	1	063.073.225.2...	1	1			1	15	10500	2005.11.14 1...
1	1	085.011.054.2...	1	1			1	2	14362	2005.11.15 1...
2	1	004.002.002.0...	2	1			1	4	96349	2005.11.13 1...
1	1	140.221.231.0...	1	1			1	2	591251	2005.11.14 1...
1	1	066.150.096.1...	1	1			1	10	597439	2005.11.15 1...
1	1	195.127.224.1...	1	1			1	14	623378	2005.11.16 1...
1	1	218.228.194.0...	1	1			1	10	638460	2005.11.14 1...
1	1	064.236.022.0...	1	1			1	10	638566	2005.11.15 1...
1	1	217.006.164.1...	1	1			1	11	828549	2005.11.14 1...
2	1	195.127.224.1...	1	1			1	26	1143702	2005.11.16 1...
1	1	140.221.130.1...	1	1			1	16	1296905	2005.11.14 1...
1	1	064.012.138.2...	1	1			1	15	6481338	2005.11.15 1...
7	1	047.129.109.1...	1	1			1	3050	15006000	2005.11.16 1...
1	1	206.024.192.2...	1	1			1	24	119212850	2005.11.15 1...
1	1	164.046.121.0...	1	1			1	70	215652317	2005.11.15 1...
2	1	065.200.212.0...	1	1			1	38	217658554	2005.11.16 1...
1	1	209.197.121.0...	1	1			1	38	372024193	2005.11.14 1...
1	1	199.239.136.2...	1	1			1	122	1001584943	2005.11.15 1...
1	1	209.124.184.1...	1	1			1	164	9033128366	2005.11.14 1...

View Raw Data

Traffic Circle

< DIP > SPORT

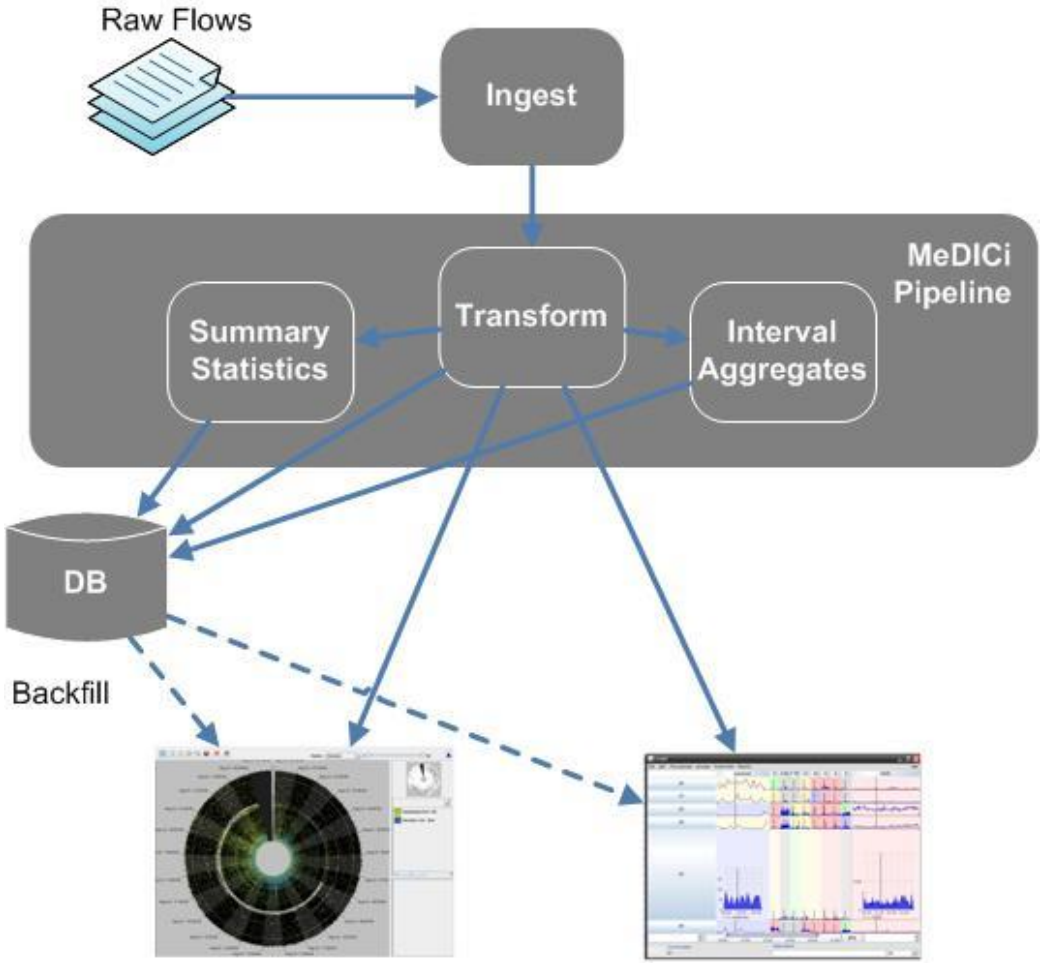
FLOWS	SIP	DIP	SPORT	DPORT	SASN	DASN	PROTO	PACKET SUM	BYTE SUM ▲	TIME
1	1	209.124.184.1...	38086	1			1	164	9033128366	2005.11.14 1...

View Raw Data

Middleware for Data-Intensive Computing (MeDICi)

- Publish and subscribe event based system
  - Published to database in addition to tools
- Components are code base agnostic
  - Easily tie in modules needed for visualizations such as aggregators and statistical analysis
- Highly scalable
  - Best run of 2781 records per second (240 million per day) on a desktop workstation (Dell 7500)

Implemented MeDICi Information Framework



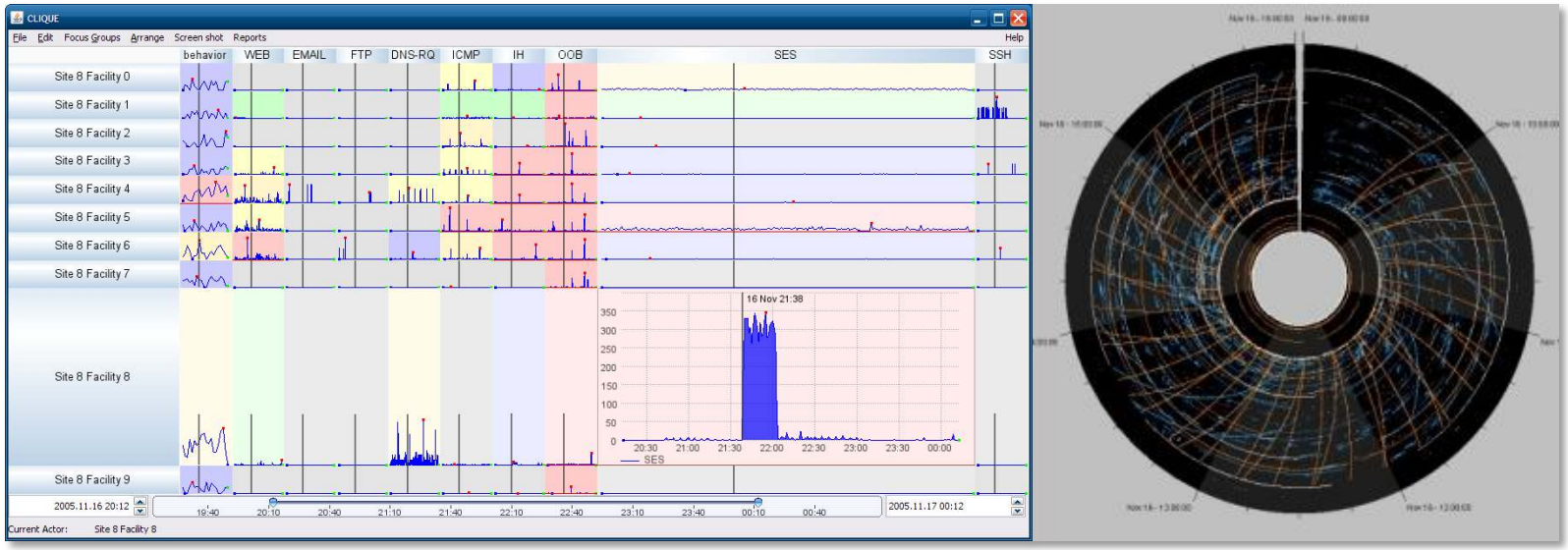
Future Directions

- Develop a predictive capability
- Explore extensions to other domains
  - Financial fraud detection
  - SCADA system reliability and security
- Enable heterogeneous data visualization
- Explore other behavioral trending algorithms

How to get in touch

Daniel Best

daniel.best@pnl.gov



Pacific Northwest
NATIONAL LABORATORY