

Pitfalls and Problems

Many ways to get visualization wrong.

Data Saturation: Our Data is Hard! (credit to Mr. Marty).

Graphics bring issues which command line tools avoid.

Tablets: Keytar of Security Visualization?

Huge push for tablets, from two directions:

Youth and Executives. Very potent combination.

Seems inevitable that we will be showing security imagery on a tablet, soon.

What about other senses? May we engage hearing or touch to better experience the data?

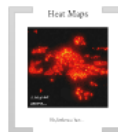
Visualization isn't about seeing, it's about understanding

Thank You.

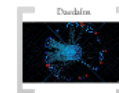
@securitytim
tray@21ct.com



Where are we going?
3D? Has to be a valid use case, but it could happen.
More annotation and grouping w/o human intervention.



Heat Maps



Desktop

Credit To The Giants

Rafael Marty - "Applied Security Visualization"
Book about the specifics of security visualization.
Ben Shneiderman - "Ten years publications in early
interaction, user interface pioneer since 1980s."
Eight Golden Rules of Interface Design (roughly there)
Shneiderman's Matrix - Overview, users and filters,
details on data and.
Maters and Clancy - "Whoever You See, See Nothing"
Best network security using ever.

Tim Ray

Amplify FCU



Department of
Information Resources,
State of Texas



21CT



@SecurityTim

Origin Systems (EA)



LYNXeon

Credit To The Giants

Rafael Marty -- "Applied Security Visualization"

Book about the specifics of security visualization.

Ben Shneiderman -- Too many publications to easily mention, user interface pioneer since 1980s.

Eight Golden Rules of Interface Design (google them!)

Shneiderman's Mantra -- Overview, zoom and filter, details on demand.

Makem and Clancy -- "Whatever You Say, Say Nothing"

Best network security song ever.

Why Visualize?

Dense Information -- Humans process visual information very fast and have discriminatory power hard to replicate in a machine.

Internal Marketing

Must convince non-technical folks

Security as elevator pitch

Art is Acquisition, Content is Retention

Overview, Zoom and Filter, Details on Demand

Lesson from Games:
Art is Acquisition,
Content is Retention

We did this backwards, IMO

It applies to everything, even netflow security.

Magazine or Broken iPad?



Overview, Zoom and Filter, Details on Demand
--Ben Shneiderman

The Way We Were

What did we do before?

Lots of spreadsheets and text files.

Not that there's anything wrong with that...

Why was that not enough?

Database search advantage.

Need to search for more than one thing at a time.

Closer to real time is better.

Note: It may be enough in your environment!

Src IP	Dst IP	Appln	Src Port	Dst Port	Protocol	DSCP	TCP FLAGS	Flow Rate	Traffic	Packets	NextHop	FNF NbarApp
192.168.10.1	192.168.13.1	compressnet	2	169	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	15.80.39.28	-
192.168.10.1	192.168.13.1	compressnet	2	564	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	190.23.69.213	-
192.168.10.1	192.168.13.1	compressnet	2	741	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	95.55.61.159	-
192.168.10.1	192.168.13.1	compressnet	281	2	TCP	AF12	UAP SF	1.0 Kbps	1.0 KB	2	223.191.78.79	-
192.168.10.1	192.168.13.1	compressnet	165	3	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	64.15.70.93	-
192.168.10.1	192.168.13.1	compressnet	424	3	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	149.191.44.148	-
192.168.10.1	192.168.13.1	compressnet	822	3	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	73.7.175.22	-
192.168.10.1	192.168.13.1	rje	800	5	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	74.157.168.220	-
192.168.10.1	192.168.13.1	discard	9	714	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	1.209.56.6	-
192.168.10.1	192.168.13.1	daytime	13	252	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	232.237.195.100	-
192.168.10.1	192.168.13.1	daytime	960	13	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	22.88.95.248	-
192.168.10.1	192.168.13.1	msp	18	116	TCP	AF12	UAP SF	1.0 Kbps	1.0 KB	2	81.203.252.131	-
192.168.10.1	192.168.13.1	msp	18	735	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	18.50.17.126	-
192.168.10.1	192.168.13.1	ftp-data	20	513	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	240.7.195.4	-

```

root@PRELAY01: ~ -- telnet -- 233x59

IPV4 SRC ADDR      IPV4 DST ADDR      TNSG SRC PORT      TNSG DST PORT      ENTP INPUT
-----
209.182.176.243    209.182.176.239    80805             2095             V11              0:00             17             0             209.182.176.11             0:00             1862             4             20:09:41:052             20:09:41:052             0:00             253             253
209.182.176.18     224.8.8.8           0                 V11              0:00             8                 0             0:0.0.0.0                   0:00             368             6             20:09:42:248             20:09:41:038             0:00             1             1
209.182.176.1     224.8.8.8           0                 Fd0              0:00             8                 0             0:0.0.0.0                   0:00             368             6             20:09:42:284             20:09:41:044             0:00             1             1
209.182.176.244    209.182.176.239    45323            2095             V11              0:00             17             0             209.182.176.11             0:00             176             3             20:09:42:042             20:09:41:040             0:00             252             252
209.182.176.244    209.182.176.239    44211            2095             V11              0:00             17             0             209.182.176.11             0:00             828             3             20:09:42:076             20:09:41:056             0:00             254             254
20:09:24:213       209.182.176.8       48313            0:00             Fd0              0:00             64             0             0:0.0.0.0                   0:00             64             1             20:09:41:952             20:09:41:952             0:00             236             236
20:09:24:213       209.182.176.2       43824            0:00             Fd0              0:00             64             0             0:0.0.0.0                   0:00             64             1             20:09:41:956             20:09:41:956             0:00             236             236
20:09:24:213       209.182.176.9       36245            0:00             Fd0              0:00             64             0             0:0.0.0.0                   0:00             64             1             20:09:42:088             20:09:42:088             0:00             236             236
20:09:24:213       209.182.176.18      38976            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:088             20:09:42:088             0:00             236             236
209.182.176.18     24.99.24.213       47028            0:00             V11              0:00             64             0             209.182.176.11             0:00             64             1             20:09:42:088             20:09:42:088             0:00             236             236
20:09:24:213       209.182.176.43      39889            0:00             Fd0              0:00             64             0             0:0.0.0.0                   0:00             64             1             20:09:42:088             20:09:42:088             0:00             236             236
20:09:24:213       209.182.176.14      33489            0:00             Fd0              0:00             64             0             0:0.0.0.0                   0:00             64             1             20:09:42:012             20:09:42:012             0:00             236             236
20:09:24:213       209.182.176.21      47172            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:028             20:09:42:028             0:00             236             236
20:09:24:213       209.182.176.18      38976            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:028             20:09:42:028             0:00             236             236
20:09:24:213       209.182.176.47      36876            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:028             20:09:42:028             0:00             236             236
209.182.176.18     24.99.24.213       0                 38976            V11              0:00             64             0             209.182.176.11             0:14             40             1             20:09:42:028             20:09:42:028             0:00             253             253
209.182.176.17     24.99.24.213       0                 36876            V11              0:00             64             0             209.182.176.11             0:14             40             1             20:09:42:028             20:09:42:028             0:00             254             254
20:09:24:213       209.182.176.22      36272            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:024             20:09:42:024             0:00             236             236
20:09:24:213       209.182.176.29      42964            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:024             20:09:42:024             0:00             236             236
20:09:24:213       209.182.176.26      44876            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:024             20:09:42:024             0:00             236             236
20:09:24:213       209.182.176.36      38807            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:024             20:09:42:024             0:00             236             236
20:09:24:213       209.182.176.25      33508            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:024             20:09:42:024             0:00             236             236
209.182.176.26     24.99.24.213       0                 44876            V11              0:00             64             0             209.182.176.11             0:14             40             1             20:09:42:024             20:09:42:024             0:00             252             252
209.182.176.28     24.99.24.213       0                 33788            V11              0:00             64             0             209.182.176.11             0:14             40             1             20:09:42:044             20:09:42:044             0:00             236             236
20:09:24:213       209.182.176.33      45134            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:044             20:09:42:044             0:00             236             236
209.182.176.33     24.99.24.213       0                 45134            V11              0:00             64             0             209.182.176.11             0:14             40             1             20:09:42:044             20:09:42:044             0:00             252             252
20:09:24:213       209.182.176.38      41388            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:048             20:09:42:048             0:00             236             236
20:09:24:213       209.182.176.41      48441            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:048             20:09:42:048             0:00             236             236
20:09:24:213       209.182.176.34      37828            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:082             20:09:42:082             0:00             236             236
20:09:24:213       209.182.176.37      47222            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:082             20:09:42:082             0:00             236             236
209.182.176.46     24.99.24.213       0                 48441            V11              0:00             64             0             209.182.176.11             0:14             40             1             20:09:42:082             20:09:42:082             0:00             251             251
20:09:24:213       209.182.176.42      42817            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:082             20:09:42:082             0:00             236             236
209.182.176.34     24.99.24.213       0                 37222            V11              0:00             64             0             209.182.176.11             0:14             40             1             20:09:42:082             20:09:42:082             0:00             251             251
20:09:24:213       209.182.176.48      36214            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:082             20:09:42:082             0:00             236             236
20:09:24:213       209.182.176.46      34811            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:082             20:09:42:082             0:00             236             236
209.182.176.42     24.99.24.213       0                 43817            V11              0:00             64             0             209.182.176.11             0:14             40             1             20:09:42:082             20:09:42:082             0:00             258             258
20:09:24:213       209.182.176.8       35978            0:00             Fd0              0:00             64             0             0:0.0.0.0                   0:00             64             1             20:09:42:082             20:09:42:082             0:00             236             236
20:09:24:213       209.182.176.13      47288            0:00             Fd0              0:00             64             0             0:0.0.0.0                   0:00             64             1             20:09:42:128             20:09:42:128             0:00             236             236
20:09:24:213       209.182.176.14      43343            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:128             20:09:42:128             0:00             236             236
20:09:24:213       209.182.176.21      34476            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:128             20:09:42:128             0:00             236             236
20:09:24:213       209.182.176.22      35484            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:128             20:09:42:128             0:00             236             236
20:09:24:213       209.182.176.29      43221            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:128             20:09:42:128             0:00             236             236
20:09:24:213       209.182.176.38      47222            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:128             20:09:42:128             0:00             236             236
20:09:24:213       209.182.176.37      36877            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:148             20:09:42:148             0:00             236             236
20:09:24:213       209.182.176.43      47407            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:148             20:09:42:148             0:00             236             236
20:09:24:213       209.182.176.45      46464            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:156             20:09:42:156             0:00             236             236
20:09:24:213       209.182.176.46      35978            0:00             Fd0              0:00             64             0             209.182.176.18             0:00             64             1             20:09:42:156             20:09:42:156             0:00             236             236
20:09:24:213       209.182.176.46      39788            0:00             Fd0              0:00             64             0             209.182.176.11             0:00             7616             109             20:09:42:168             20:09:42:168             0:00             236             236
20:09:24:213       209.182.176.37      41848            0:00             Fd0              0:00             64             0             209.182.176.11             0:00             7616             119             20:09:42:168             20:09:42:168             0:00             236             236
20:09:24:213       209.182.176.429      38850            0:00             Fd0              0:00             64             0             209.182.176.11             0:00             7852             118             20:09:42:168             20:09:42:168             0:00             236             236
20:09:24:213       209.182.176.44      46468            0:00             Fd0              0:00             64             0             209.182.176.11             0:00             7852             128             20:09:42:168             20:09:42:168             0:00             236             236
20:09:24:213       209.182.176.46      35978            0:00             Fd0              0:00             64             0             209.182.176.11             0:00             7852             128             20:09:42:168             20:09:42:168             0:00             236             236
20:09:24:213       209.182.176.147      39988            0:00             Fd0              0:00             64             0             209.182.176.11             0:00             7852             128             20:09:42:168             20:09:42:168             0:00             236             236
20:09:24:213       209.182.176.134      42813            0:00             Fd0              0:00             64             0             209.182.176.11             0:00             7408             117             20:09:42:168             20:09:42:168             0:00             236             236
20:09:24:213       209.182.176.125      27888            0:00             Fd0              0:00             64             0             209.182.176.11             0:00             7408             117             20:09:42:168             20:09:42:168             0:00             236             236
20:09:24:213       209.182.176.148      37638            0:00             Fd0              0:00             64             0             209.182.176.11             0:00             7408             117             20:09:42:168             20:09:42:168             0:00             236             236

```

The Way We Were

What did we do before?

Lots of spreadsheets and text files.

Not that there's anything wrong with that...

Why was that not enough?

Database search advantage.

Need to search for more than one thing at a time.

Closer to real time is better.

Note: It may be enough in your environment!

What are we Doing Now?

Graphs

The screenshot displays the LYNXeon Analyst Studio interface. The main window shows a complex network graph with numerous nodes and connecting lines. A context menu is open over a central node, listing various actions such as 'Expand...', 'Expansion Queries', 'Delete', and 'Properties'. The interface includes a menu bar (File, Edit, Data, Search, View, Window, Help), a toolbar with search and navigation icons, and a status bar at the bottom showing 'Completed: Refreshing the result sets 00:00.78'. The graph nodes are represented by globe icons, and the connections are thin lines radiating from a central point.

LYNXeon Analyst Studio

File Edit Data Search View Window Help

Active Project: Cyber - 21ct-netcap 2 Search connections from: 10.0.10.165 to: 10.0.10.165 Search Advanced Search:

Quick Tips *MDL (NetworkAddress) *Cyber - 21ct-netcap 2 - Untitled Cyber - 21ct-netcap 2 Analytic Catalog *Cyber - 21ct-netcap 2 - Untitled *Searching Connections

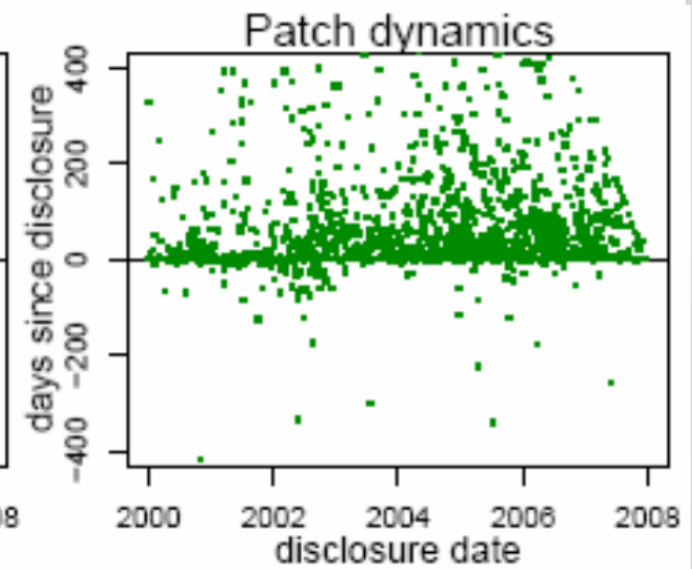
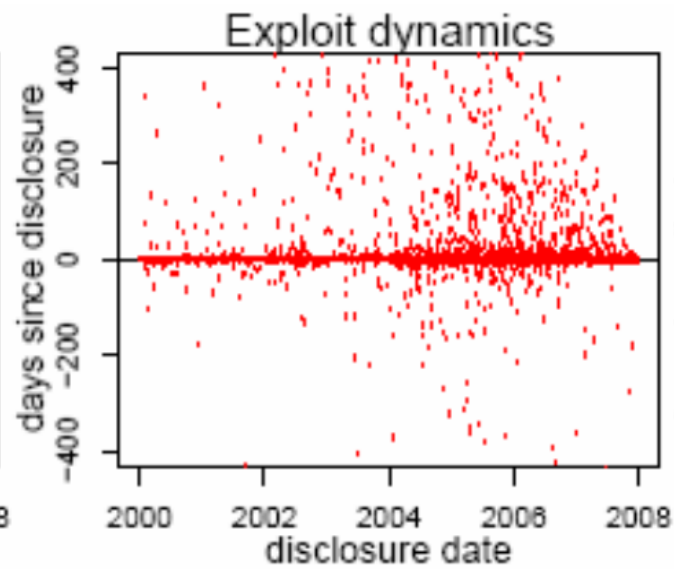
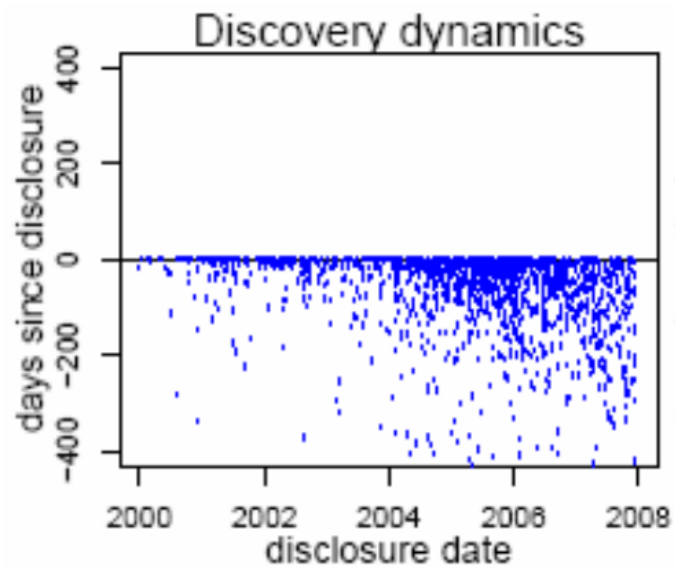
Expand...
Expansion Queries
Expand Relations
Search Other Sources
Advanced Analysis
Link To Entities By Attribute
Create Search Pattern
Geospatial References
Geospatial Analysis
Tagging
Add Database Entity
Add Connecting Relation
Edit Database Properties
Merge Nodes
Delete
Find...
Select
Edit Custom Styles
Arrange
Zoom
Print Preview
Copy Diagram to Clipboard
Export
Revisions
Properties

Link Filter Timeline Simplify Paths Combine Parallel Links Apply Grouping Rules

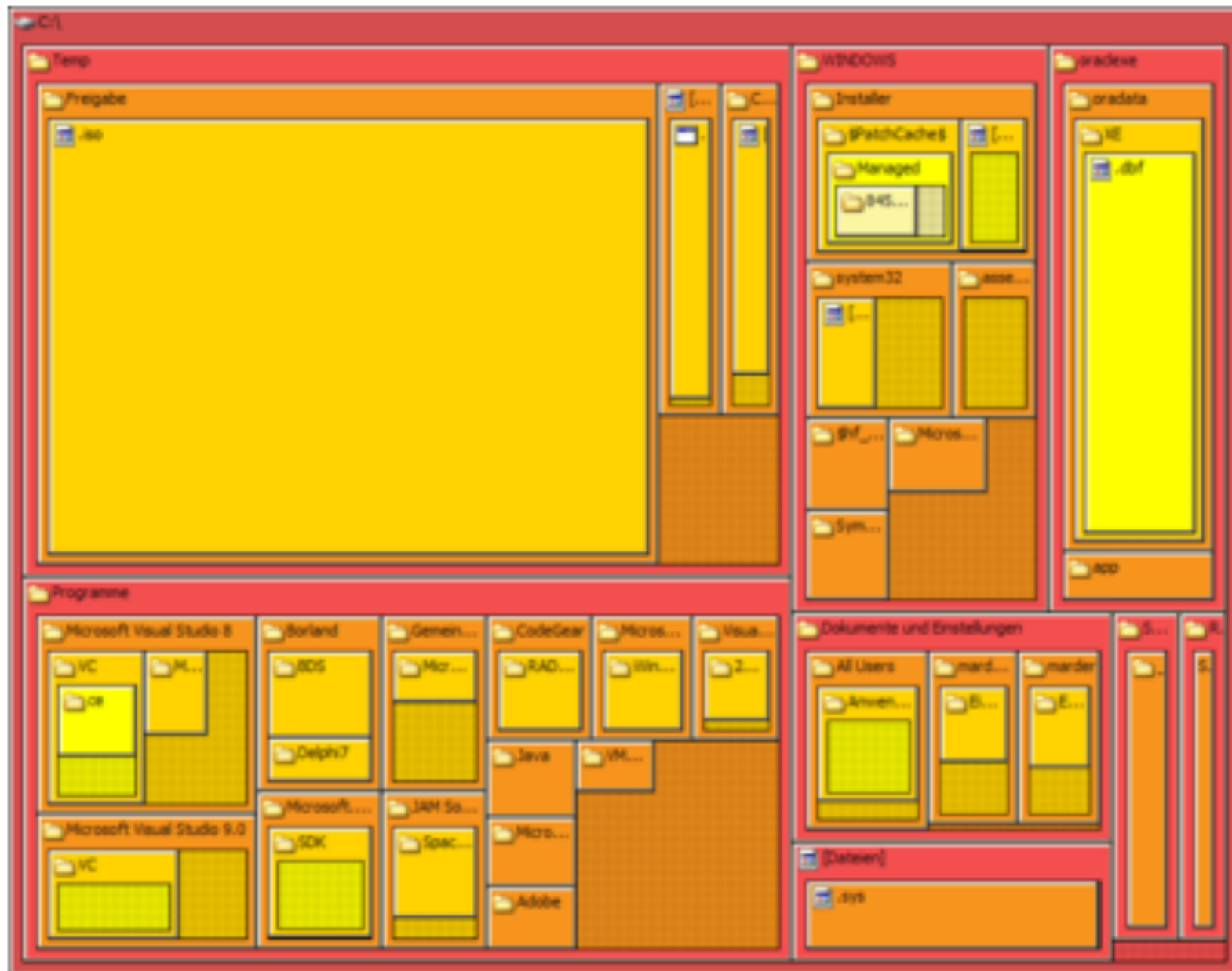
Diagram Table Metrics

Completed: Refreshing the result sets 00:00.78

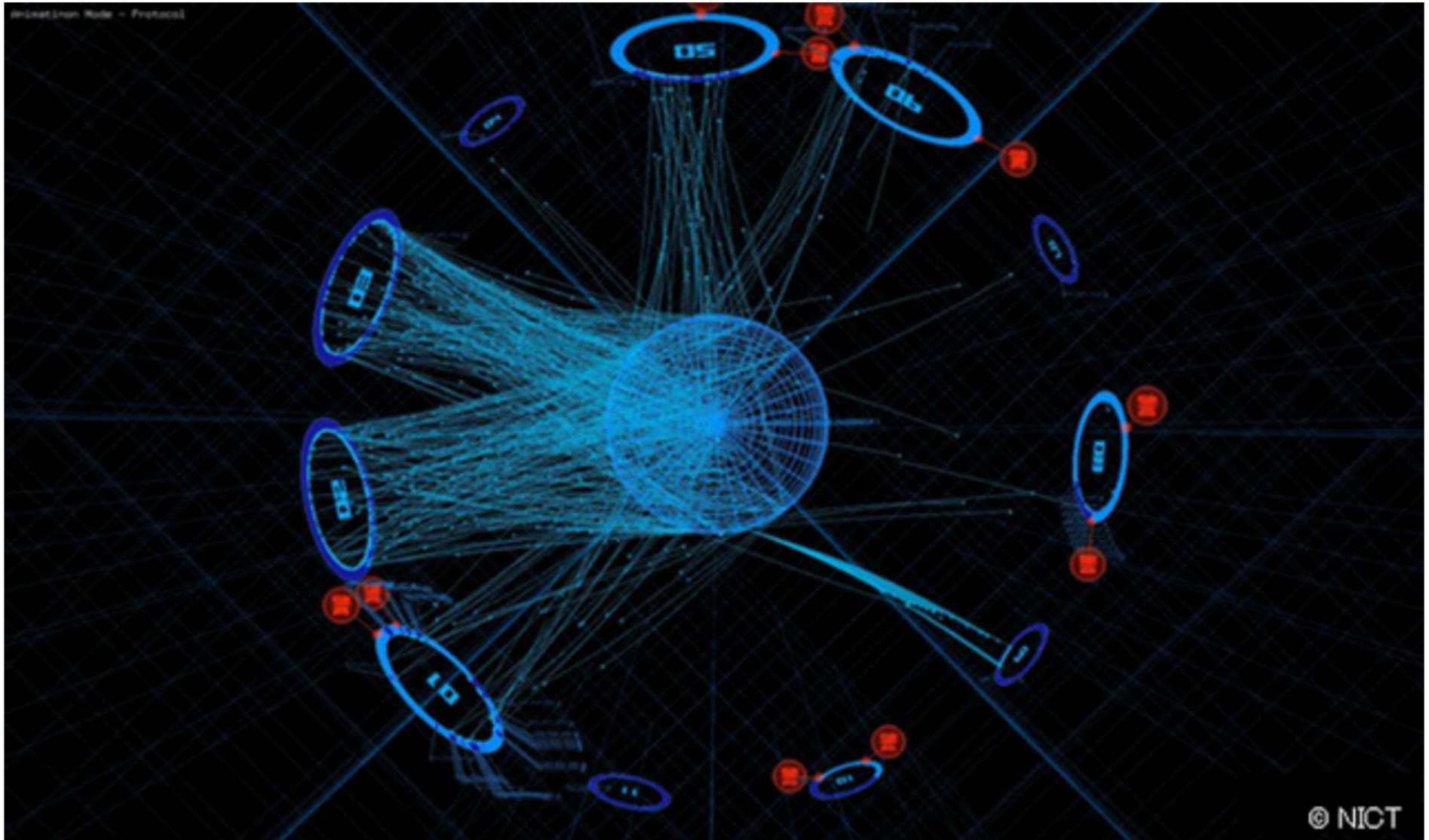
Scatter Plots



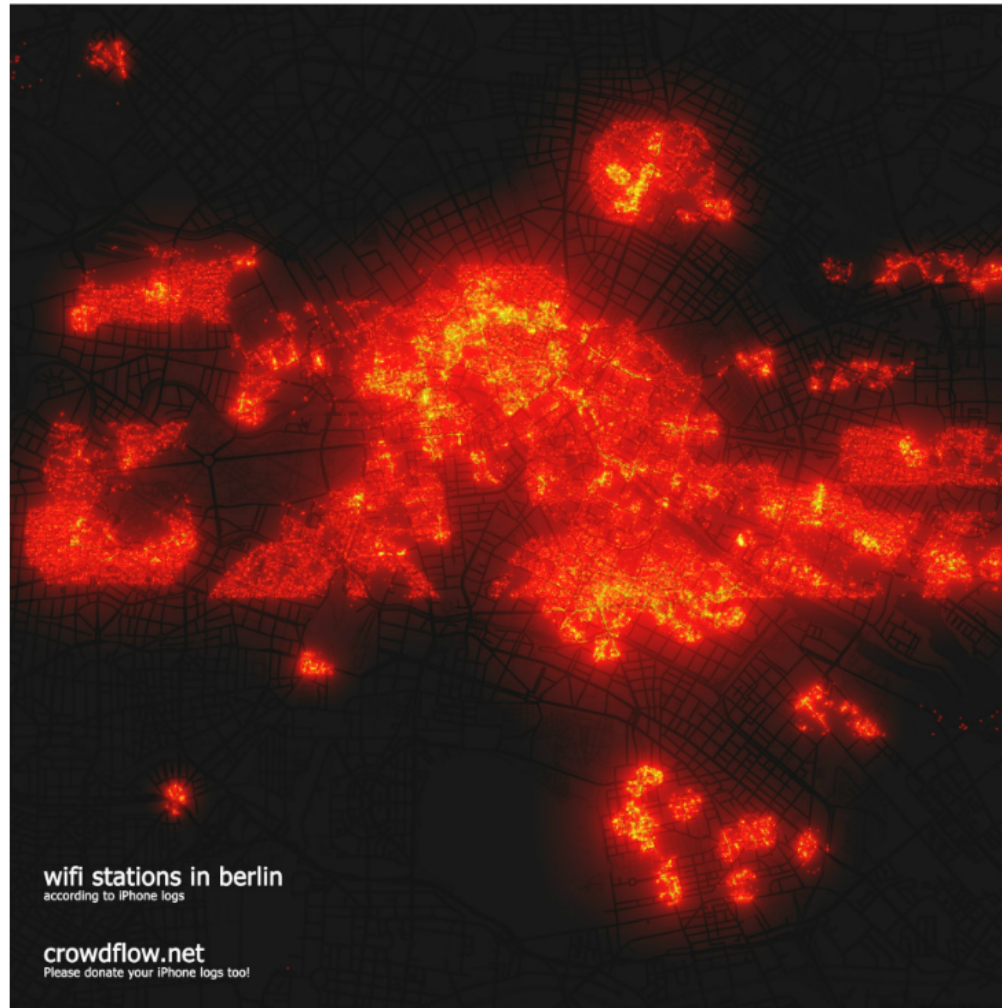
Treemaps



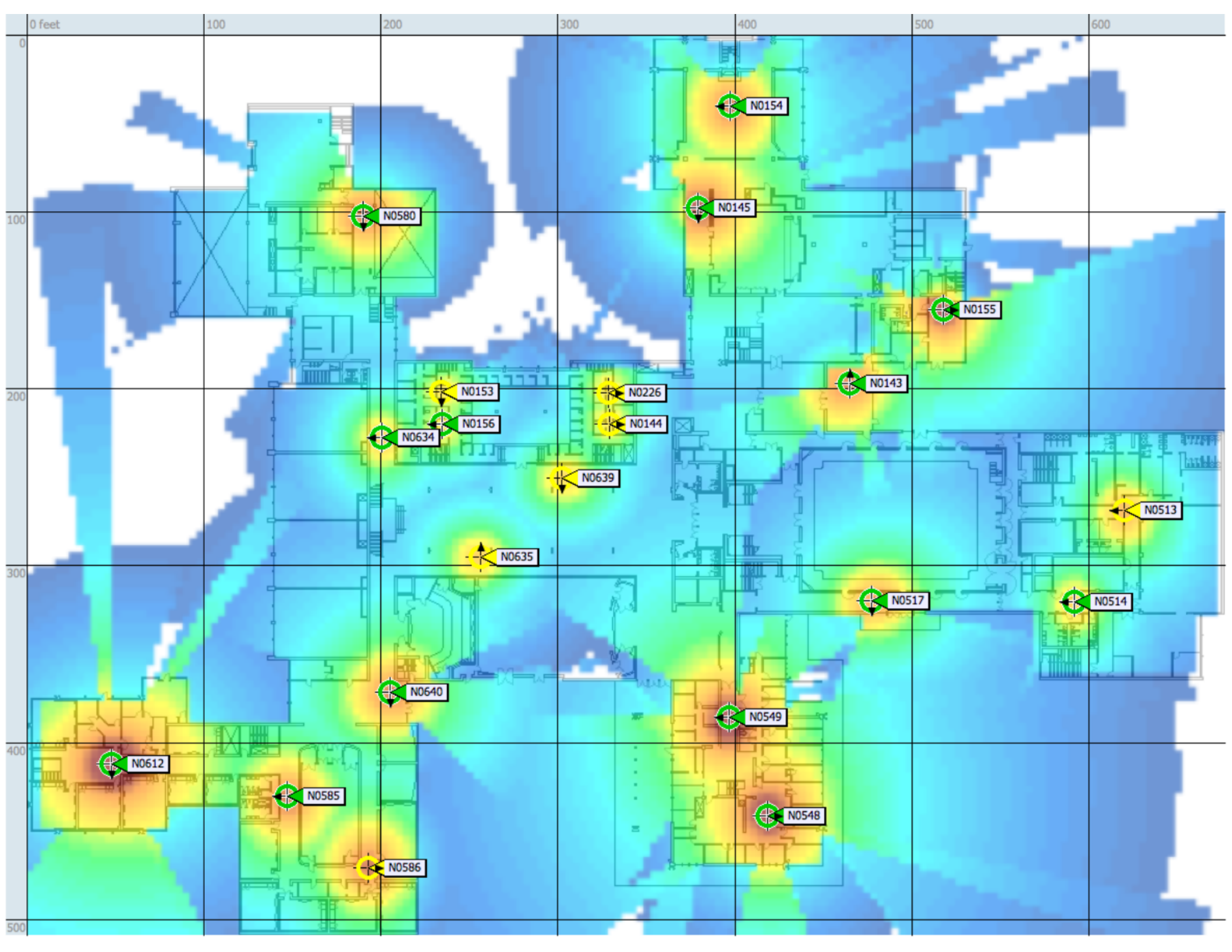
Daedalus



Heat Maps



Ok, little too hot...



0 feet

100

200

300

400

500

600

0

100

200

300

400

500

N0154

N0580

N0145

N0155

N0153

N0226

N0143

N0634

N0156

N0144

N0639

N0513

N0635

N0517

N0514

N0640

N0549

N0612

N0585

N0548

N0586



Where are we going?

3D? Has to be a valid use case, but it could happen.

More automation and grouping w/o human intervention.

Tablets: Keytar of Security Visualization?

Huge push for tablets, from two directions:

Youth and Executives. Very potent combination.

Seems inevitable that we will be showing security imagery on a tablet, soon.

What about other senses? May we engage hearing or touch to better experience the data?

Visualization isn't about seeing, it's about understanding







Pitfalls and Problems

Many ways to get visualization wrong.

Data Saturation: Our Data is Hard! (credit to Mr. Marty).

Graphics bring issues which command line tools avoid.

Thank You.

@securitytim

tray@21ct.com