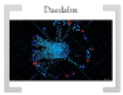
Pitfalls and Problems
Many ways to get visualization wrong.
Data Saturation: Our Data is Hard! (credit to Mr. Marty).
Graphics bring issues which command line tools avoid.

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



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.

Makers and Clancy -- "Whatever You Say, Say Nothing"
Best network security song ever.

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

Heat Maps

Dashlets

Tim Ray

Amplify FCU

Department of Information Resources, State of Texas

21CT

@SecurityTim

Origin Systems (EA)

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

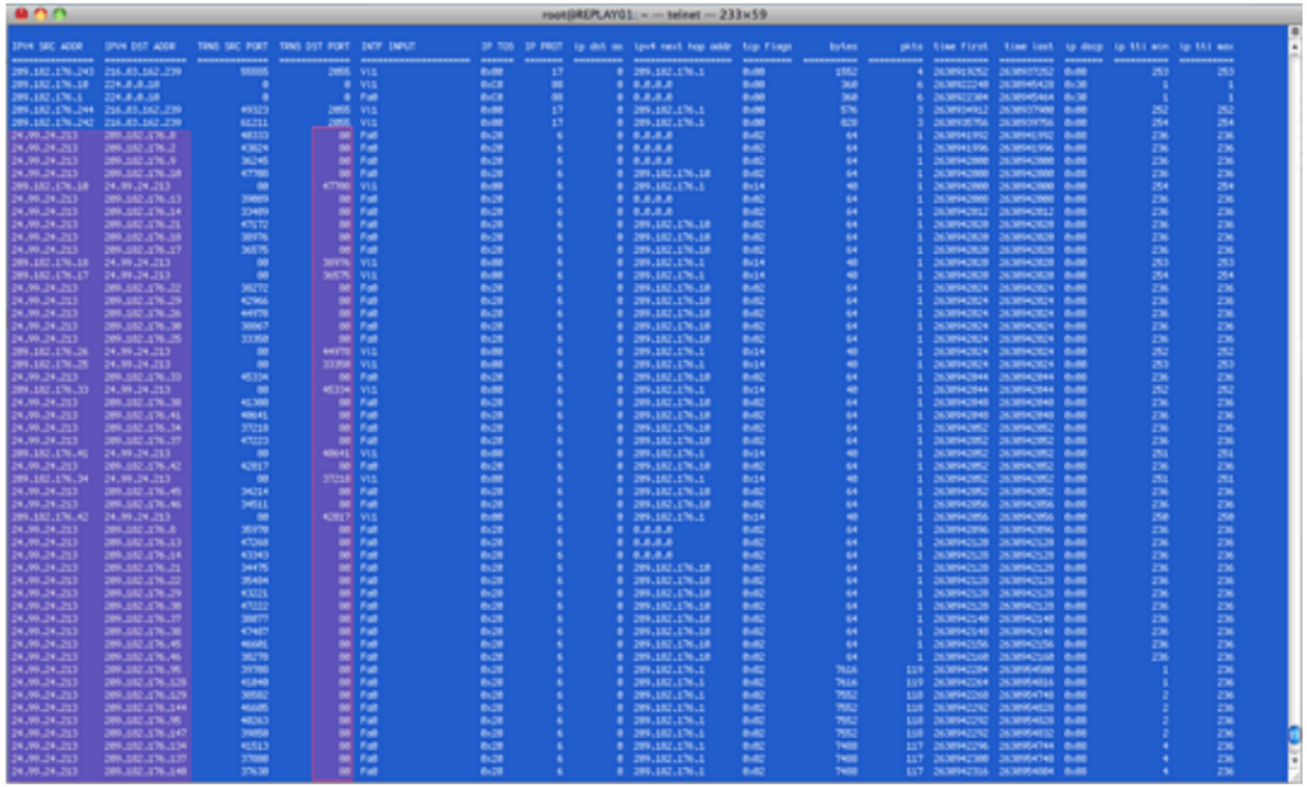
--Ben Shneiderman

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.	192.168.13.1	compressnet	2	169	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	15.80.39.28	-
192.168.10.	192.168.13.1	compressnet	2	564	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	190.23.69.213	-
192.168.10.	192.168.13.1	compressnet	2	741	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	95.55.61.159	-
192.168.10.	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.	192.168.13.1	compressnet	165	3	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	64.15.70.93	-
192.168.10.	192.168.13.1	compressnet	424	3	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	149.191.44.148	-
192.168.10.	192.168.13.1	compressnet	822	3	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	73.7.175.22	-
192.168.10.	192.168.13.1	rje	800	5	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	74.157.168.220	-
192.168.10.	192.168.13.1	discard	9	714	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	1.209.56.6	-
192.168.10.	192.168.13.1	daytime	13	252	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	232.237.195.100	-
192.168.10.	192.168.13.1	daytime	960	13	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	22.88.95.248	-
192.168.10.	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.	192.168.13.1	msp	18	735	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	18.50.17.126	-
192.168.10.	192.168.13.1	ftp-data	20	513	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	240.7.195.4	-



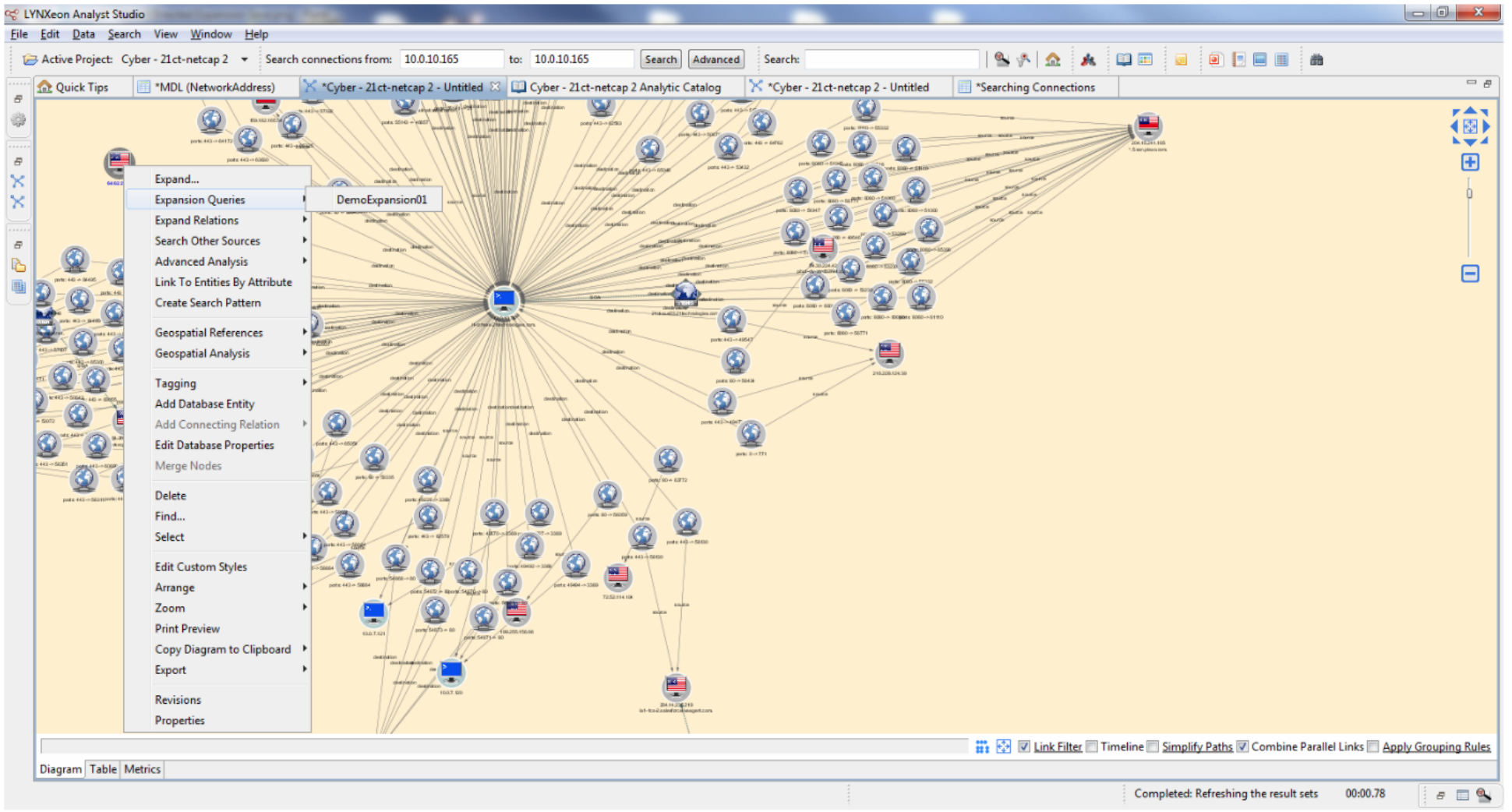
The Way We Were
What did we do before?
Lots of spreadsheets and text files.

Not that there's anything wrong with that…

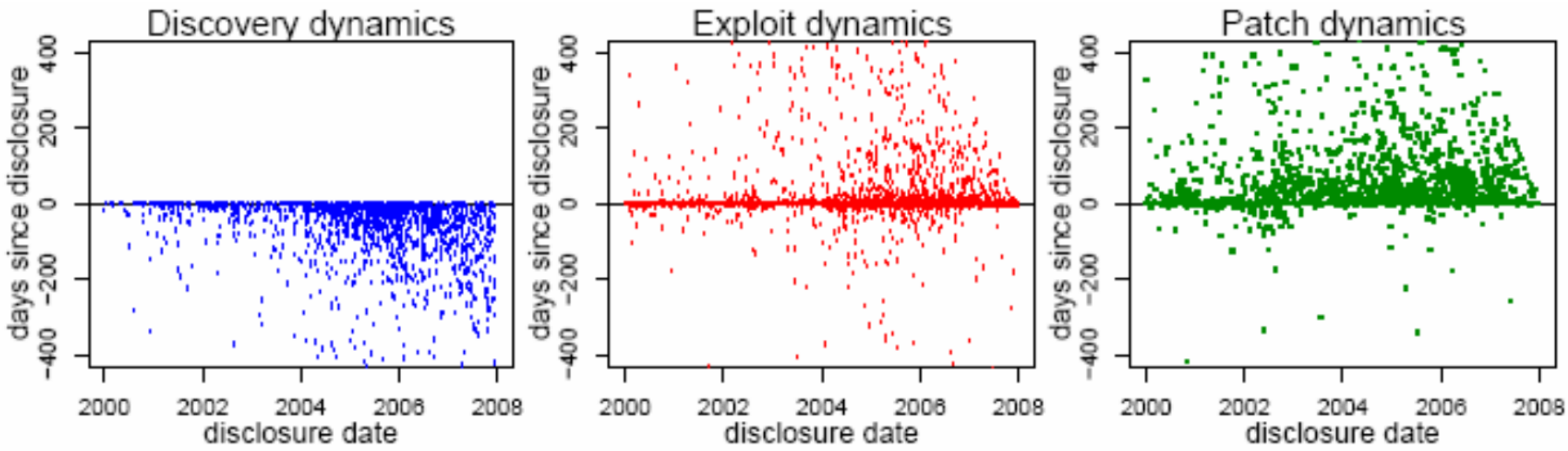
Why was that not enough?
Database search advantage.
Need to search for more than one thing at a time.
Closer to real time is better.
Note: It may be enough in your environment!

What are we Doing Now?

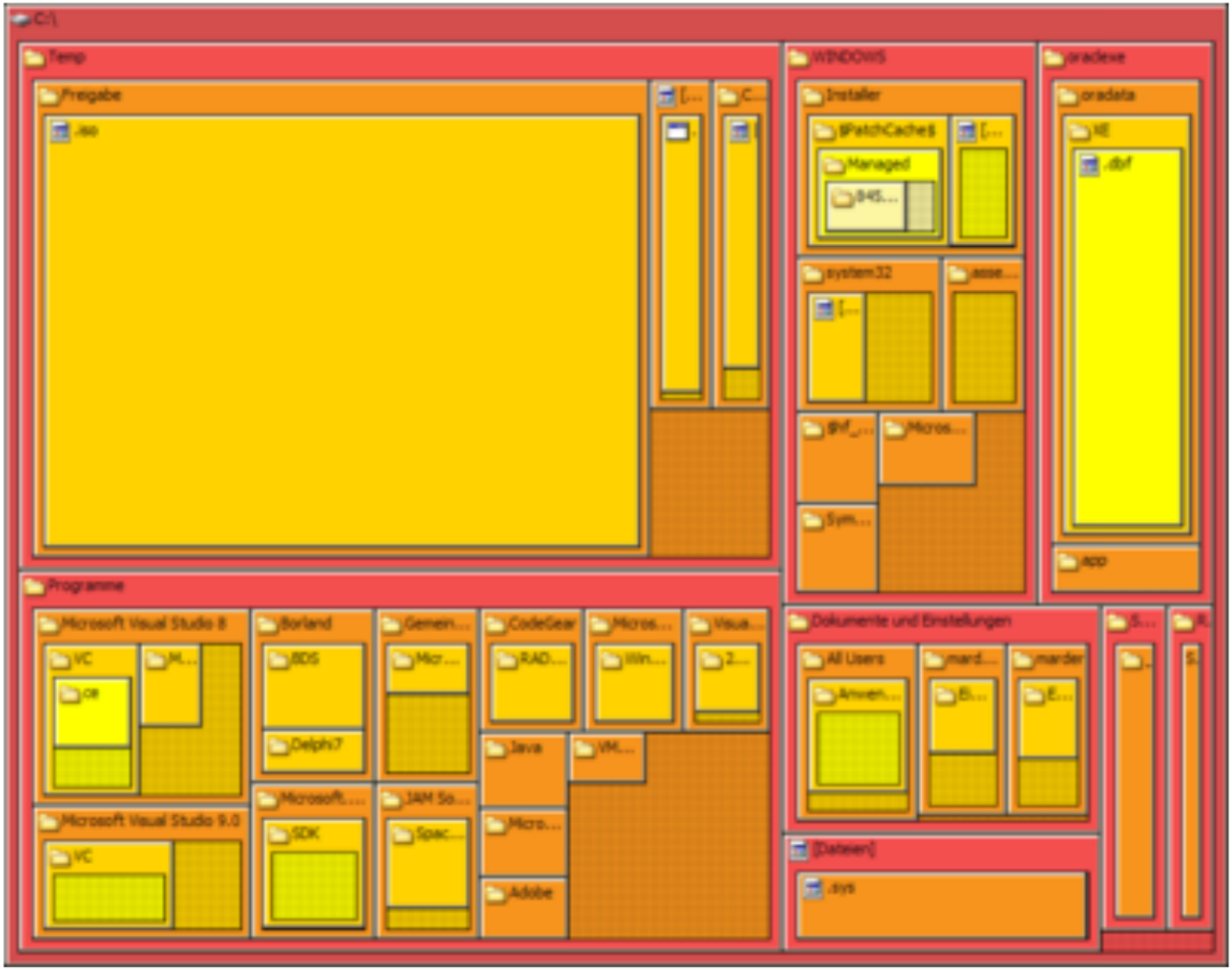
Graphs


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
DemoExpansion01
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

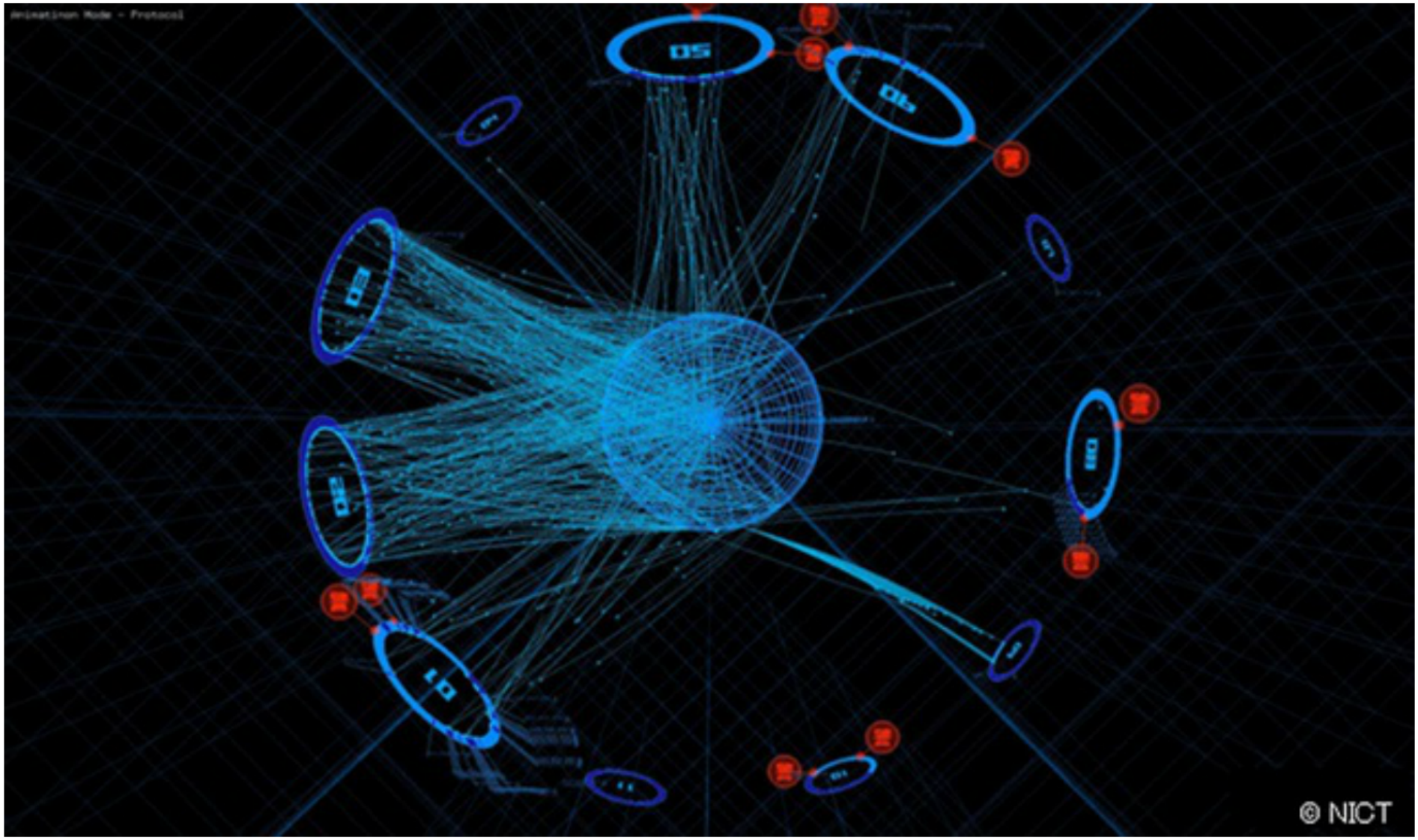
Scatter Plots



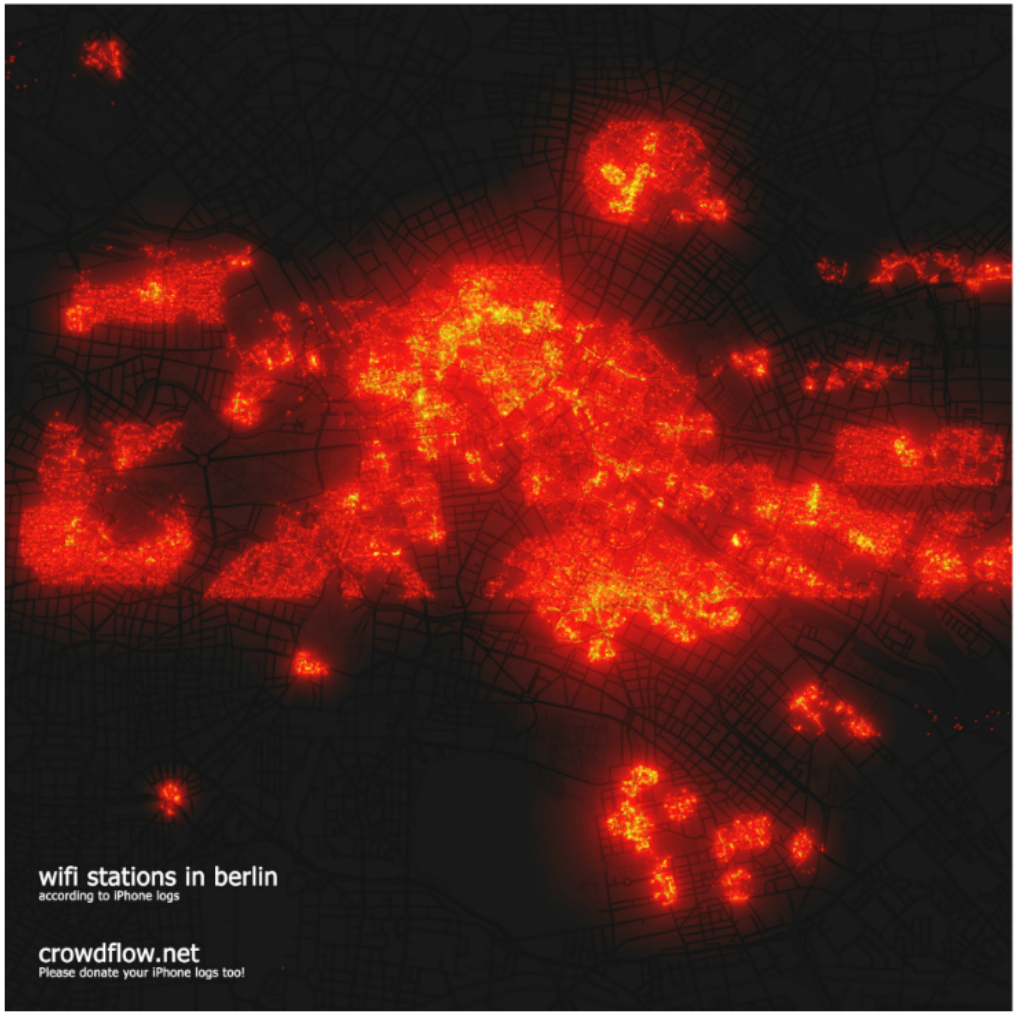
Treemaps


C:\
Temp
Freigabe
.iso
WINDOWS
Installer
$PatchCache$
Managed
system32
oracleve
oradata
.dbf
app
Programme
Microsoft Visual Studio 8
VC
Borland
BDS
Delphi7
Microsoft Visual Studio 9.0
VC
SDK
Java
Dokumente und Einstellungen
All Users
[Dateien]
.sys

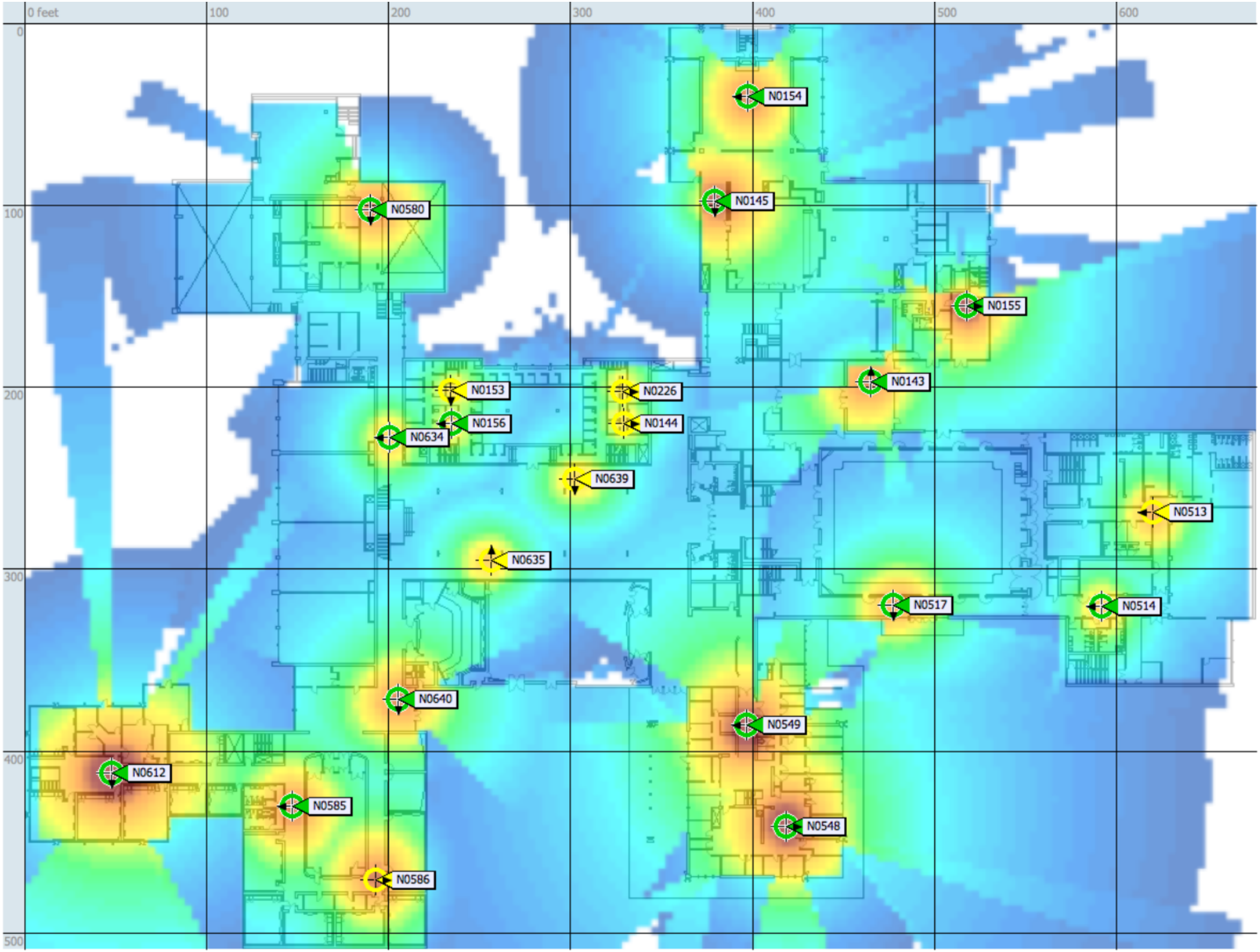
Daedalus



Heat Maps



Ok, little too hot...


0 feet
100
200
300
400
500
600
0
100
200
300
400
500
N0154
N0145
N0580
N0155
N0143
N0153
N0226
N0156
N0144
N0634
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


AT&T 3G
3:30 PM
Wednesday
23
Messages
Calendar
Photos
Camera
YouTube
Stocks
Maps
Weather
Notes
Utilities
iTunes
App Store
Settings
Phone
Mail
Safari
iPod
iPhone


TETRIS
CNN
HBO GO
epi
GUITAR HERO


Roland
Roland

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