Tools and Techniques for the Analysis of Large Scale BGP Datasets

Manish Karir, Larry Blunk (Merit)

Dion Blazakis, John Baras (UMd)

The Problem

- Large amounts of data are now, or soon will be available:
  - RouteViews, RIPE Archives, PREDICT, etc
- The problem is no longer access to raw data but how to extract useful information from the raw data
- Need tools that can:
  - Scale to large input datasets
  - Provide useful data summarizations
  - Are easy to use
  - Provide useful information
- BGP::Inspect
  - Goal is to attempt to make it easier to use raw data from archives such as RouteViews, by pre-processing, reformatting and indexing the data

Outline

- BGP::Inspect and BGPdb
  - Architecture, Techniques, Algorithms
- BGP::Inspect Interface
  - Basic queries, Global Summarizations
  - Detailed specific queries, AS/Prefix
- Case Study 1 – The AS9121 Incident
- Case Study 2 – Prefix Hijacking Example
- Conclusions, Future Work and Discussion

BGP::Inspect

- Analyzing MRT Data:
  - Large volumes of data ~RV-66G compressed
  - Extracting useful information requires writing custom parsers even for basic information
  - Lots and lots of redundancy
- Approach:
  - Preprocess RouteViews data
  - Remove redundancy as much as possible
  - Use data compression to the extent possible
  - Build efficient indices to help queries
  - Pre-compute and store commonly used statistics at data load time not at query time
  - Build easy to use interface

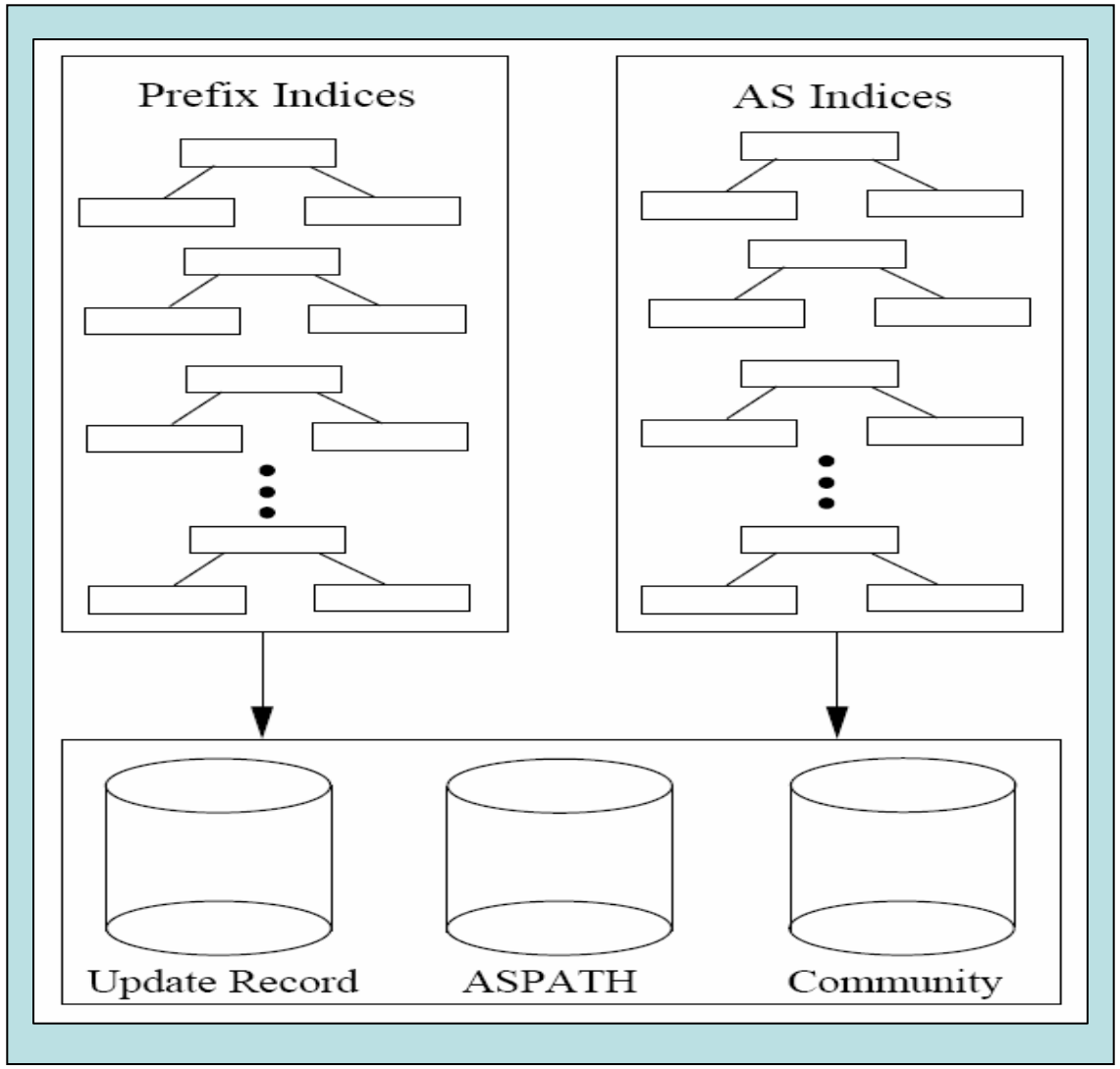
BGPdb

- BGPdb is the core of the BGP::Inspect system
- BGPdb represents the pre-processed database, which is queried by the BGP::Inspect interface
- Provides some useful techniques that maybe applied to processing other large datasets not just BGP datasets

BGPdb – Techniques and Algorithms

- Removing redundancy from BGP datasets
  - ASPATH, COMMUNITY, UPDATE Msgs are repeated over and over, only time changes
- Compressed-Chunked Files
  - Compromise between size and usability
- B+ Tree indices
  - Indexing based on time, this enables fast time-range queries
- Caching while processing input datasets
  - Messages are repetitive, so keep cache of previous processing for speedup

BGPdb – System Architecture

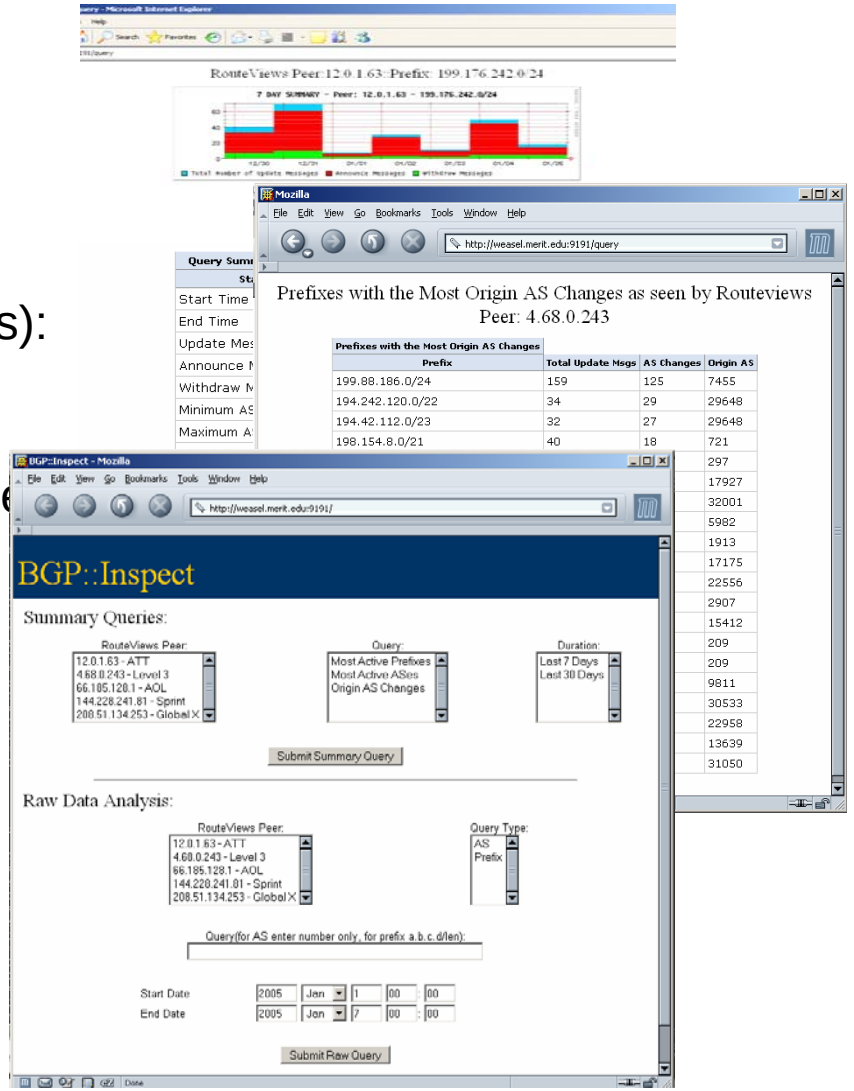


BGP::Inspect

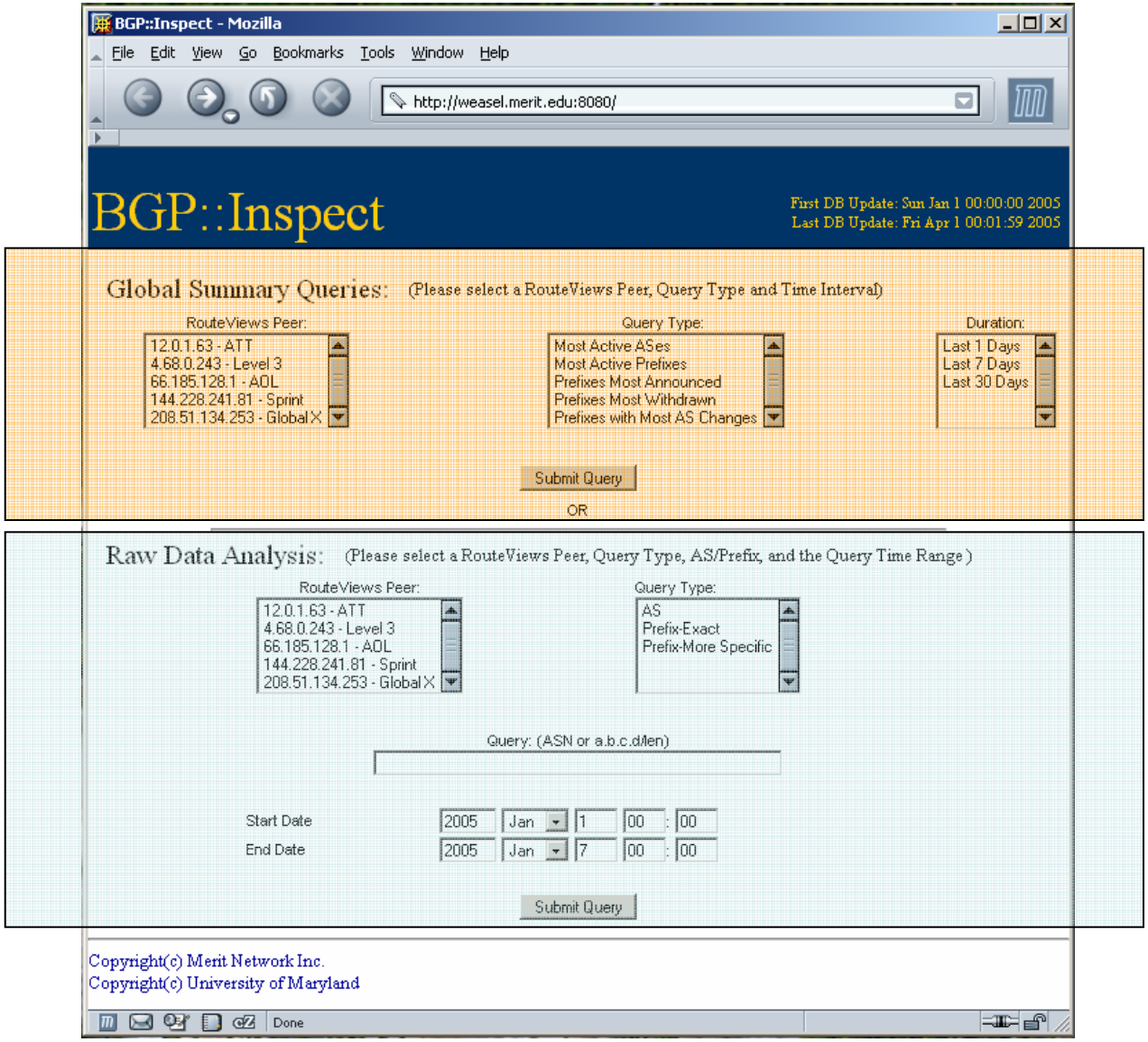
BGP::Inspect – Beta v0.2
http://weasel.merit.edu:8080

Dataset: Jan1- March31 2005

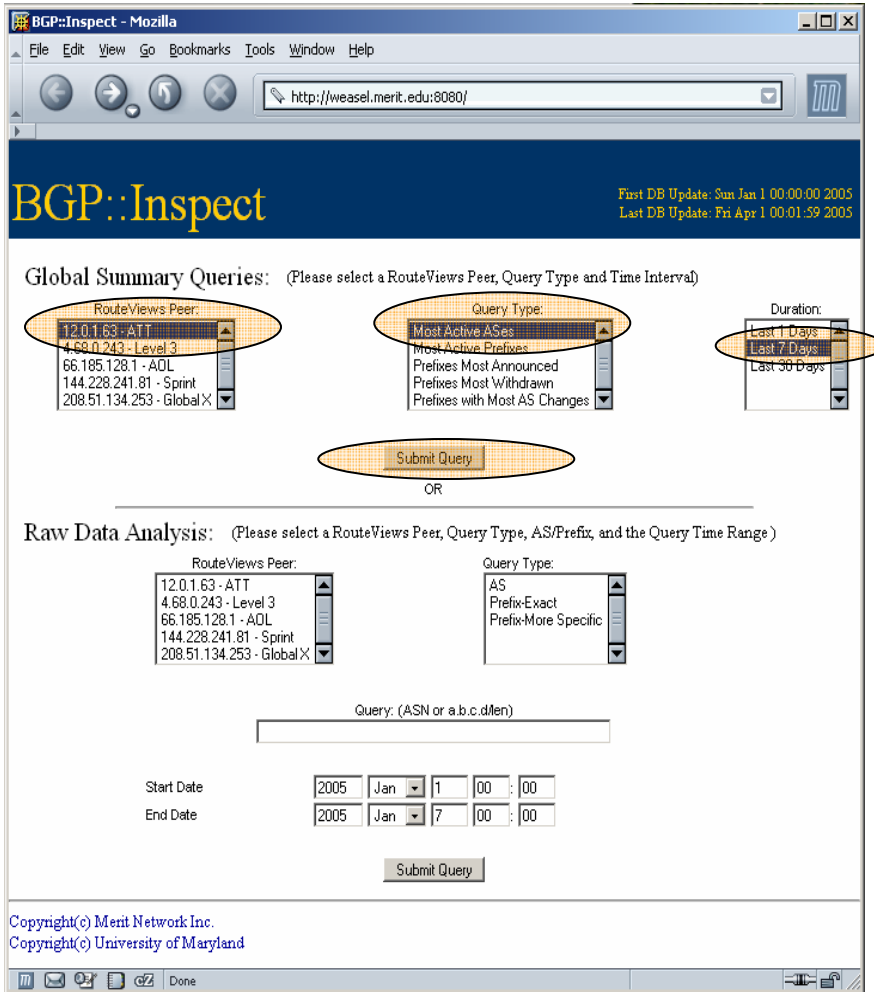
- Example queries (per peer, 1,7,30 days):
  - Most active AS's
  - Most active prefixes
  - Prefixes with most OriginAS change
- Raw Data Analysis(per peer)
  - Prefix/AS, Time Range
  - Uniques prefixes by AS
  - OriginAS changes for a prefix
  - Time to run query
  - More specific prefixes announced



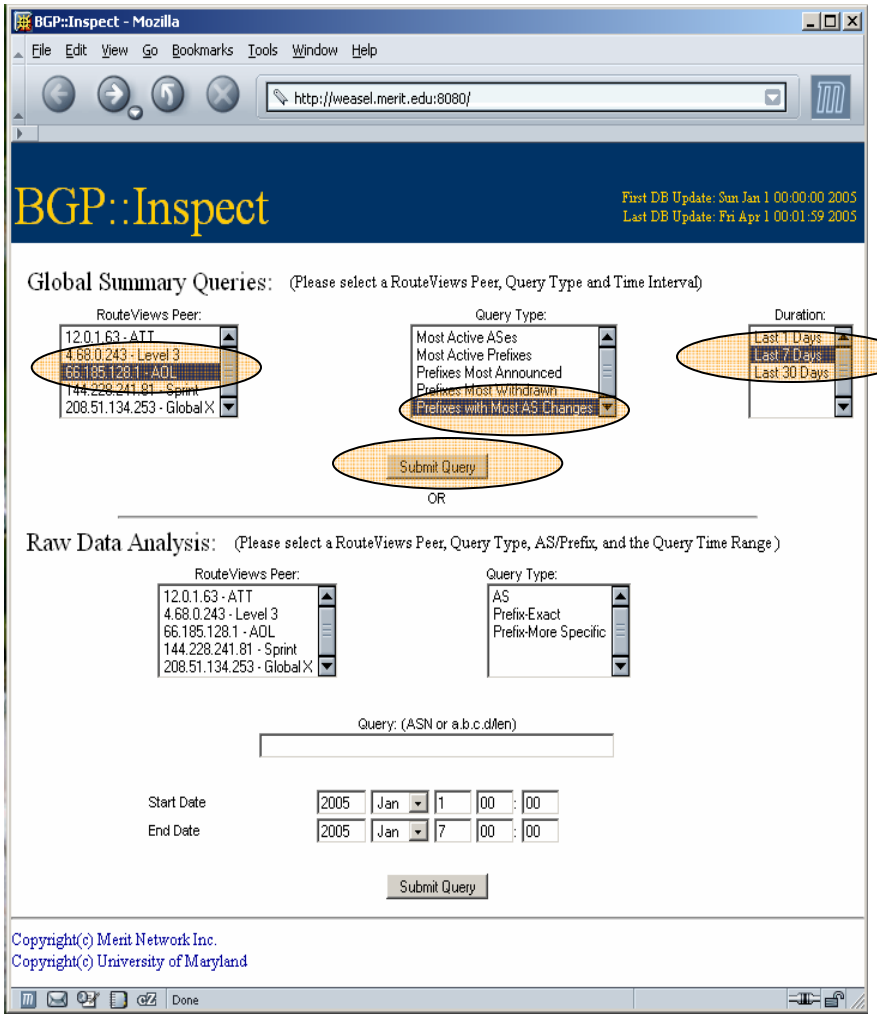
BGP::Inspect Interface

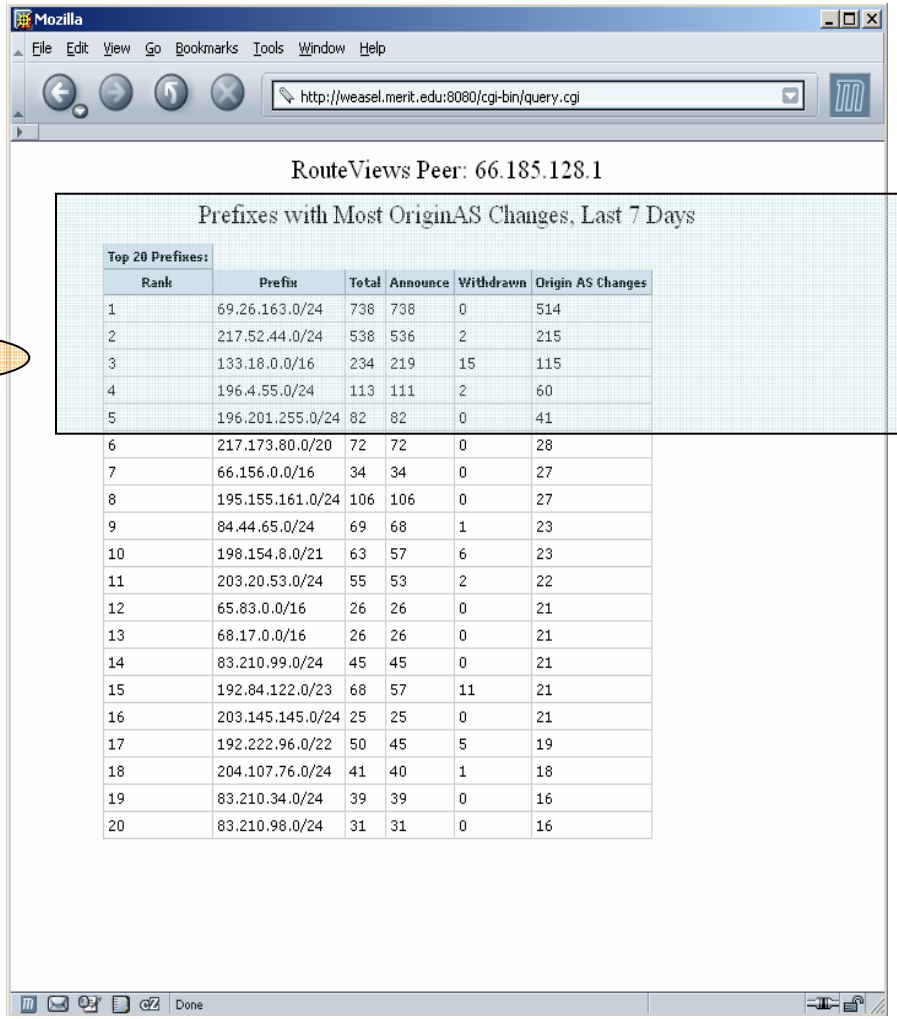


Global Queries – Most Active ASes

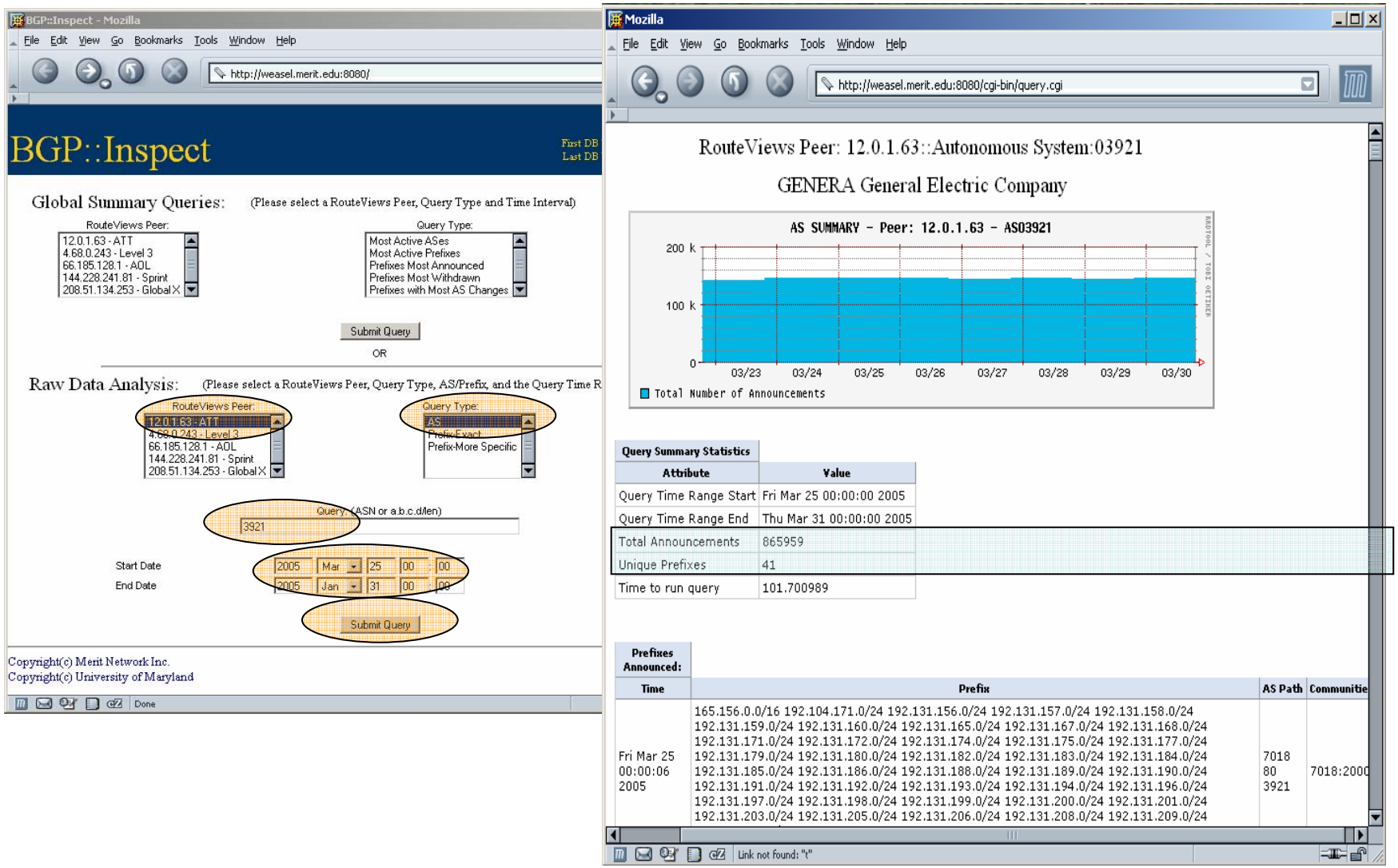


Global Queries: Most OriginAS Changes

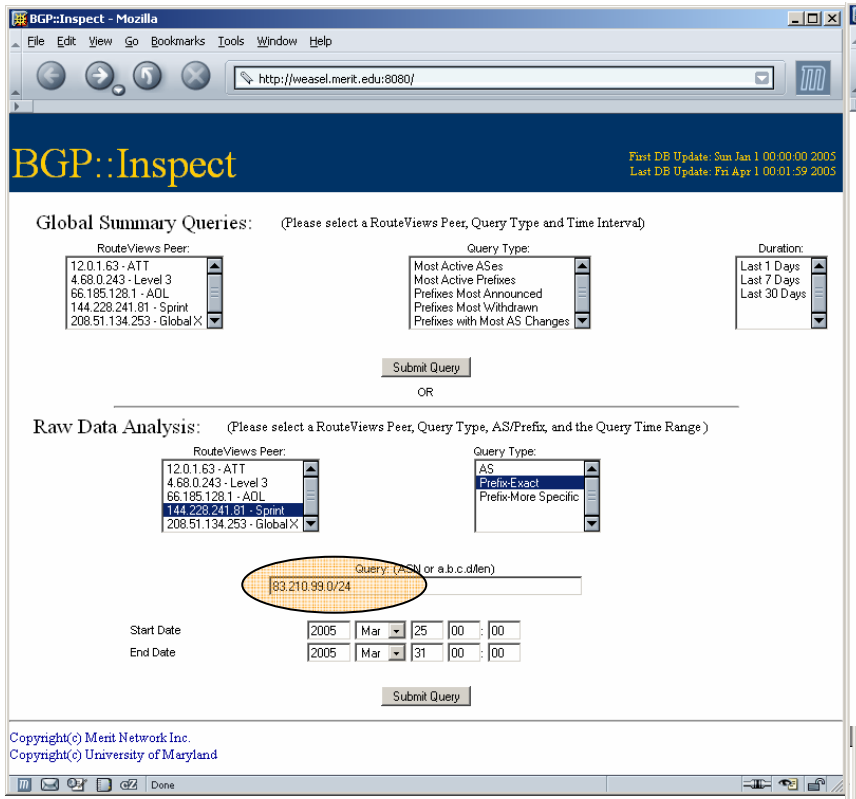


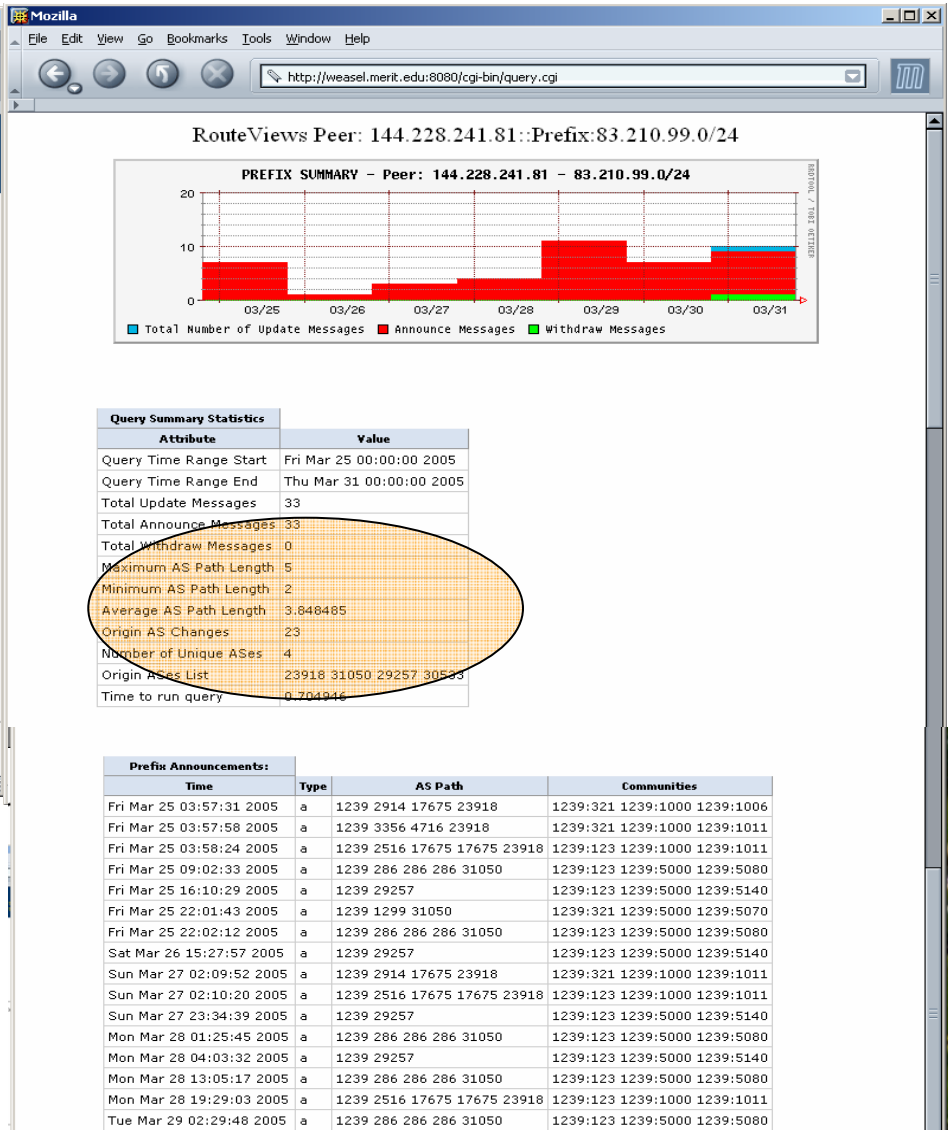


Raw Data Analysis – AS Query



Raw Data Analysis – Prefix query

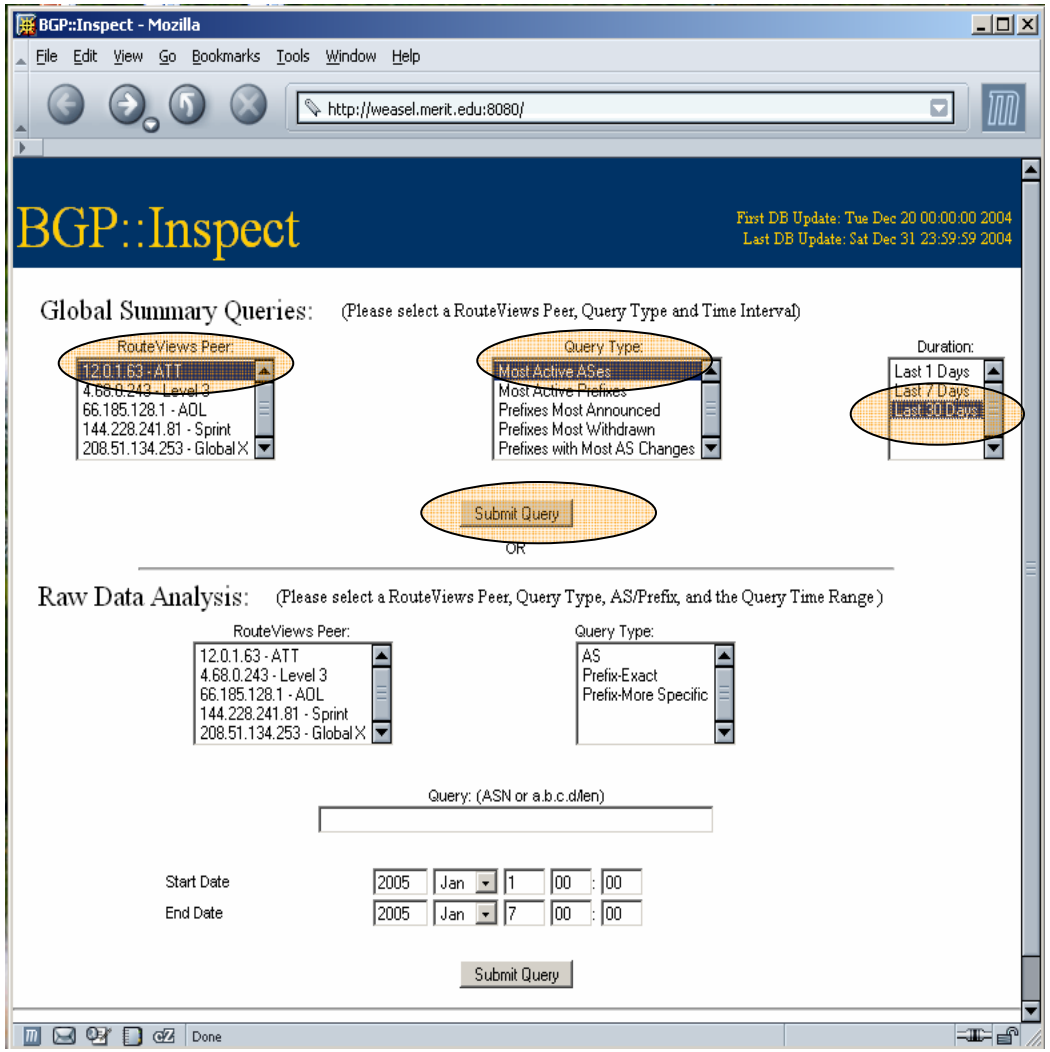




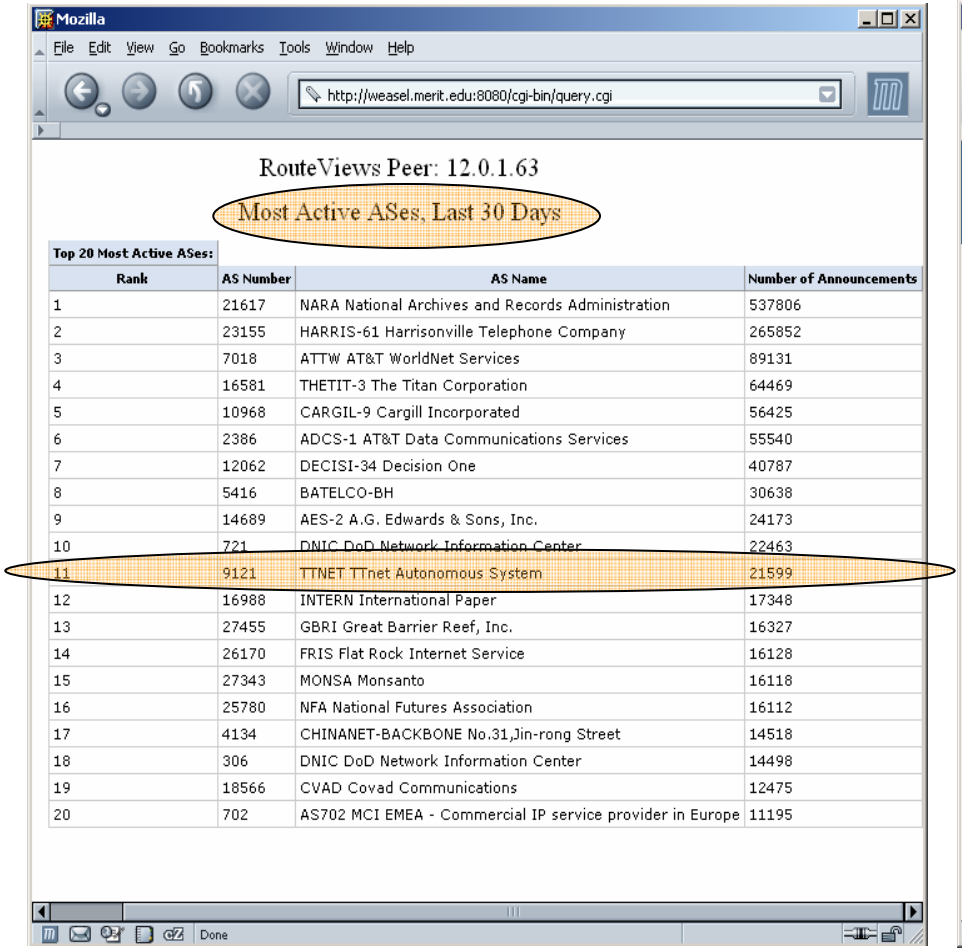
Case Study 1 – AS9121 Incident

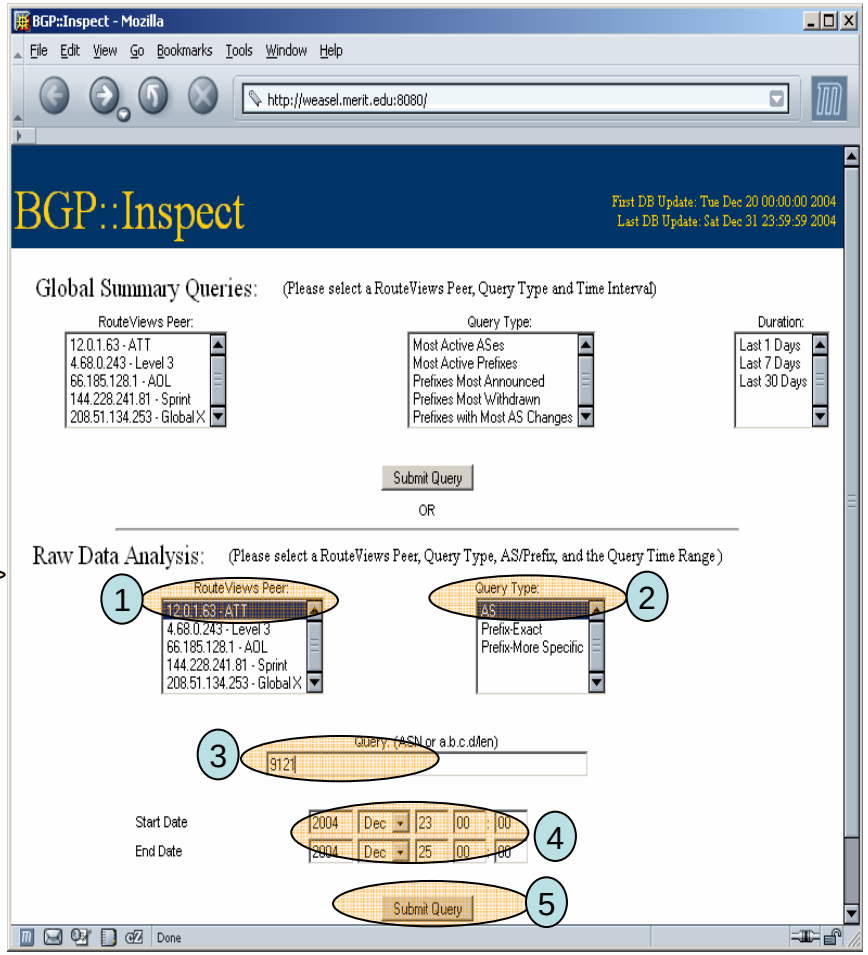
- At ~09:19 UTC on Dec 24, 2004, AS9121 began re-originating a large number of globally routed prefixes

- Forensics:
  - What happened?
  - Who did it?
  - Could there have been some early detection?
  - How widespread was it?

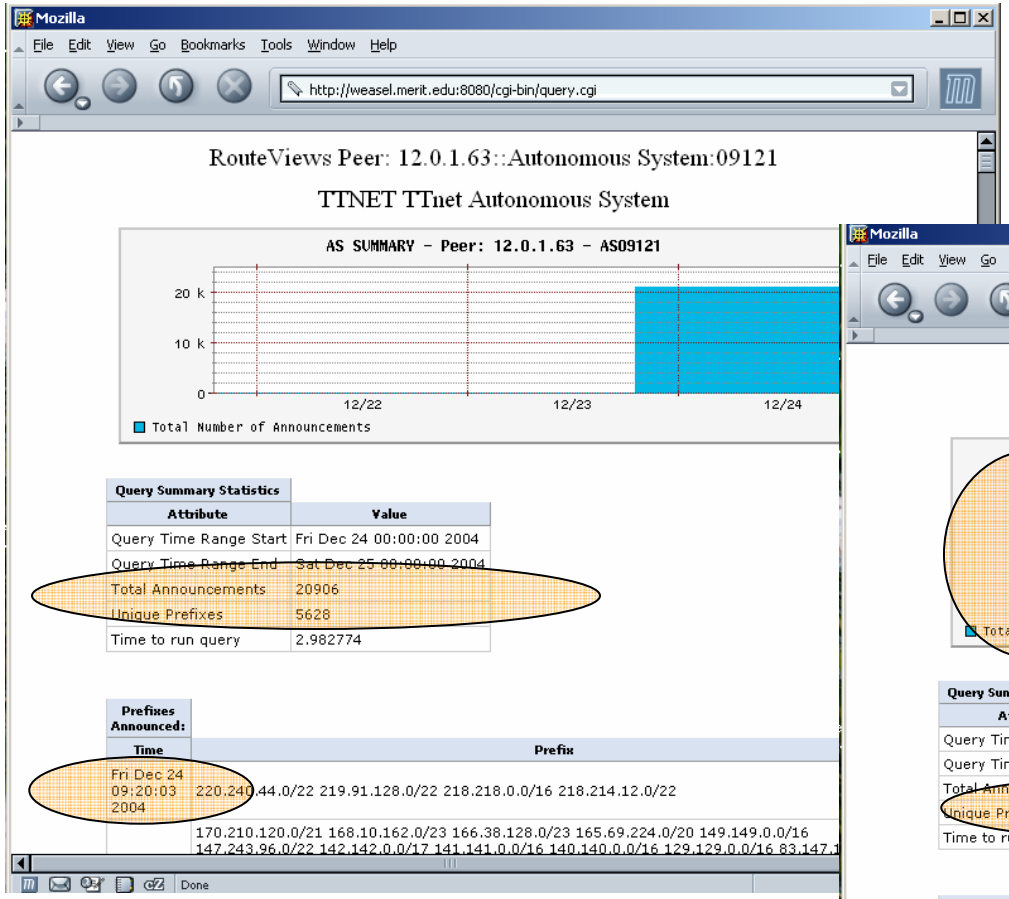


Step 1: What…


Mozilla
File Edit View Go Bookmarks Tools Window Help
http://weasel.merit.edu:8080/cgi-bin/query.cgi
RouteViews Peer: 12.0.1.63
Most Active ASes, Last 30 Days
Top 20 Most Active ASes:
Rank | AS Number | AS Name | Number of Announcements
1 | 21617 | NARA National Archives and Records Administration | 537806
2 | 23155 | HARRIS-61 Harrisonville Telephone Company | 265852
3 | 7018 | ATTW AT&T WorldNet Services | 89131
4 | 16581 | THETIT-3 The Titan Corporation | 64469
5 | 10968 | CARGIL-9 Cargill Incorporated | 56425
6 | 2386 | ADCS-1 AT&T Data Communications Services | 55540
7 | 12062 | DECISI-34 Decision One | 40787
8 | 5416 | BATELCO-BH | 30638
9 | 14689 | AES-2 A.G. Edwards & Sons, Inc. | 24173
10 | 721 | DNIC DoD Network Information Center | 22463
11 | 9121 | TTNET TTnet Autonomous System | 21599
12 | 16988 | INTERN International Paper | 17348
13 | 27455 | GBRI Great Barrier Reef, Inc. | 16327
14 | 26170 | FRIS Flat Rock Internet Service | 16128
15 | 27343 | MONSA Monsanto | 16118
16 | 25780 | NFA National Futures Association | 16112
17 | 4134 | CHINANET-BACKBONE No.31,Jin-rong Street | 14518
18 | 306 | DNIC DoD Network Information Center | 14498
19 | 18566 | CVAD Covad Communications | 12475
20 | 702 | AS702 MCI EMEA - Commercial IP service provider in Europe | 11195
Done

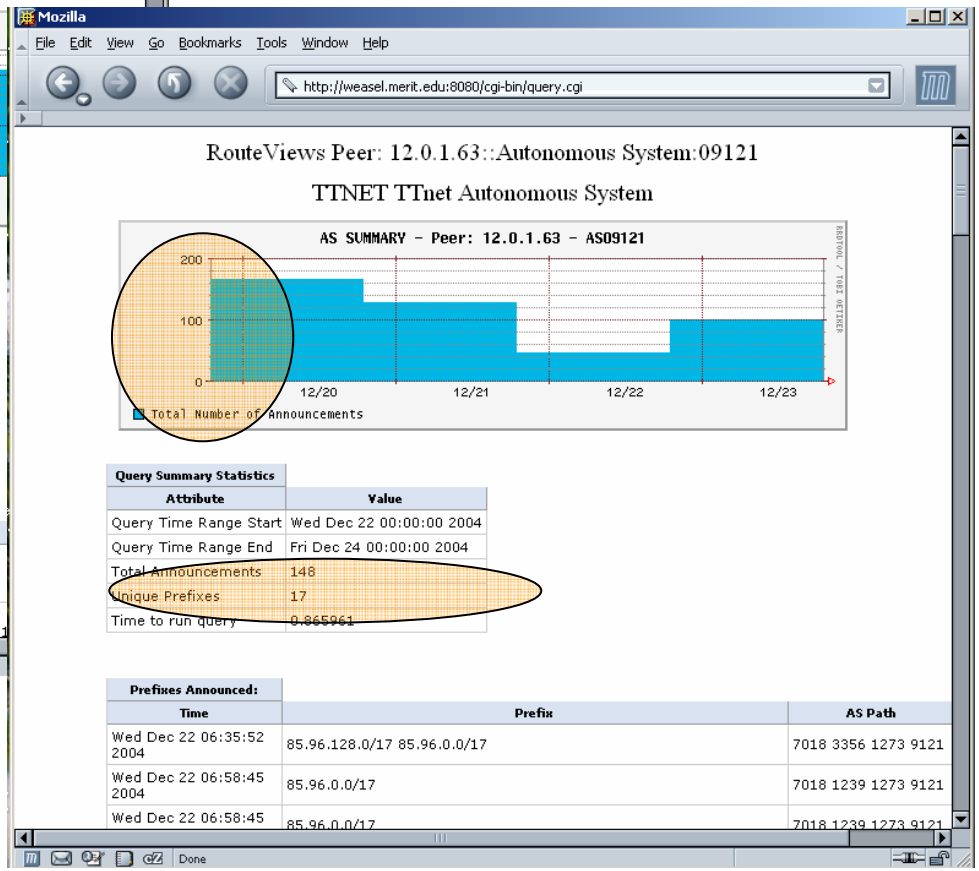

BGP::Inspect - Mozilla
File Edit View Go Bookmarks Tools Window Help
http://weasel.merit.edu:8080/
BGP::Inspect
First DB Update: Tue Dec 20 00:00:00 2004
Last DB Update: Sat Dec 31 23:59:59 2004
Global Summary Queries: (Please select a RouteViews Peer, Query Type and Time Interval)
RouteViews Peer:
12.0.1.63 - ATT
4.68.0.243 - Level 3
66.185.128.1 - AOL
144.228.241.81 - Sprint
208.51.134.253 - GlobalX
Query Type:
Most Active ASes
Most Active Prefixes
Prefixes Most Announced
Prefixes Most Withdrawn
Prefixes with Most AS Changes
Duration:
Last 1 Days
Last 7 Days
Last 30 Days
Submit Query
OR
Raw Data Analysis: (Please select a RouteViews Peer, Query Type, AS/Prefix, and the Query Time Range)
1
2
Prefix-Exact
Prefix-More Specific
3
Query: (ASN or a.b.c.d/len)
9121
Start Date
End Date
2004 Dec 23 00 00
2004 Dec 25 00 00
4
Submit Query
5
Done

Step 1.5: Hmm…interesting…

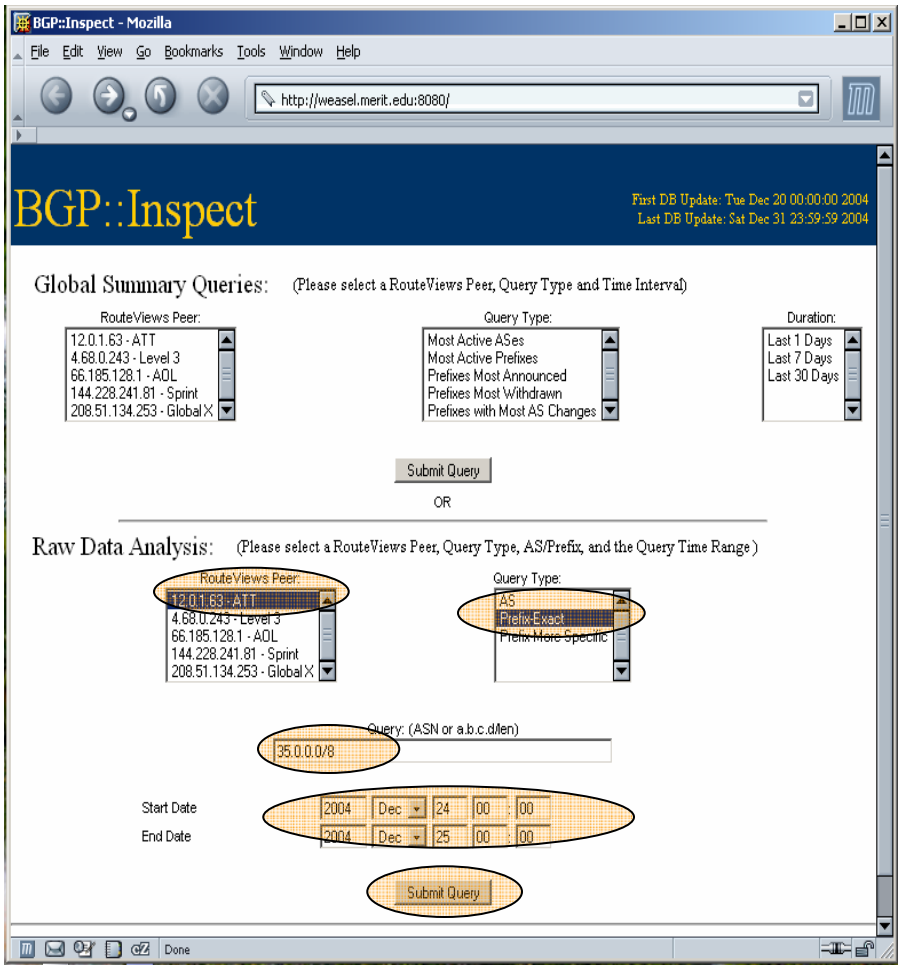


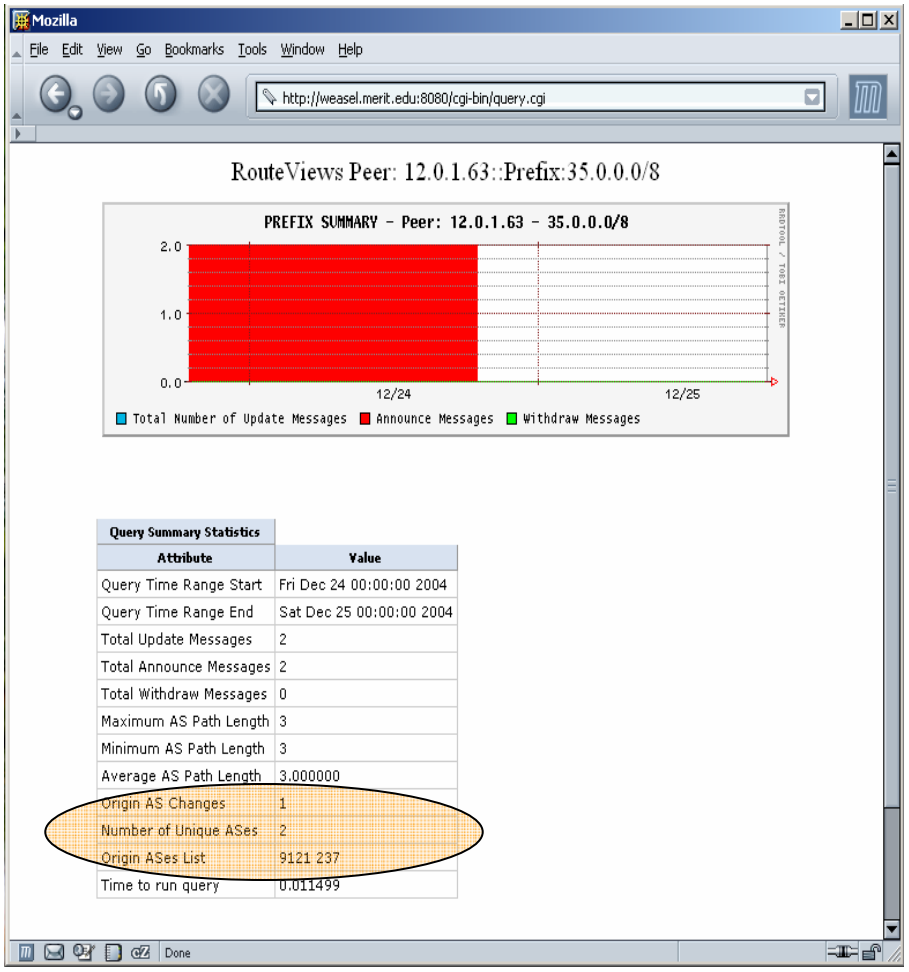
Dec 24

Dec 22, 23

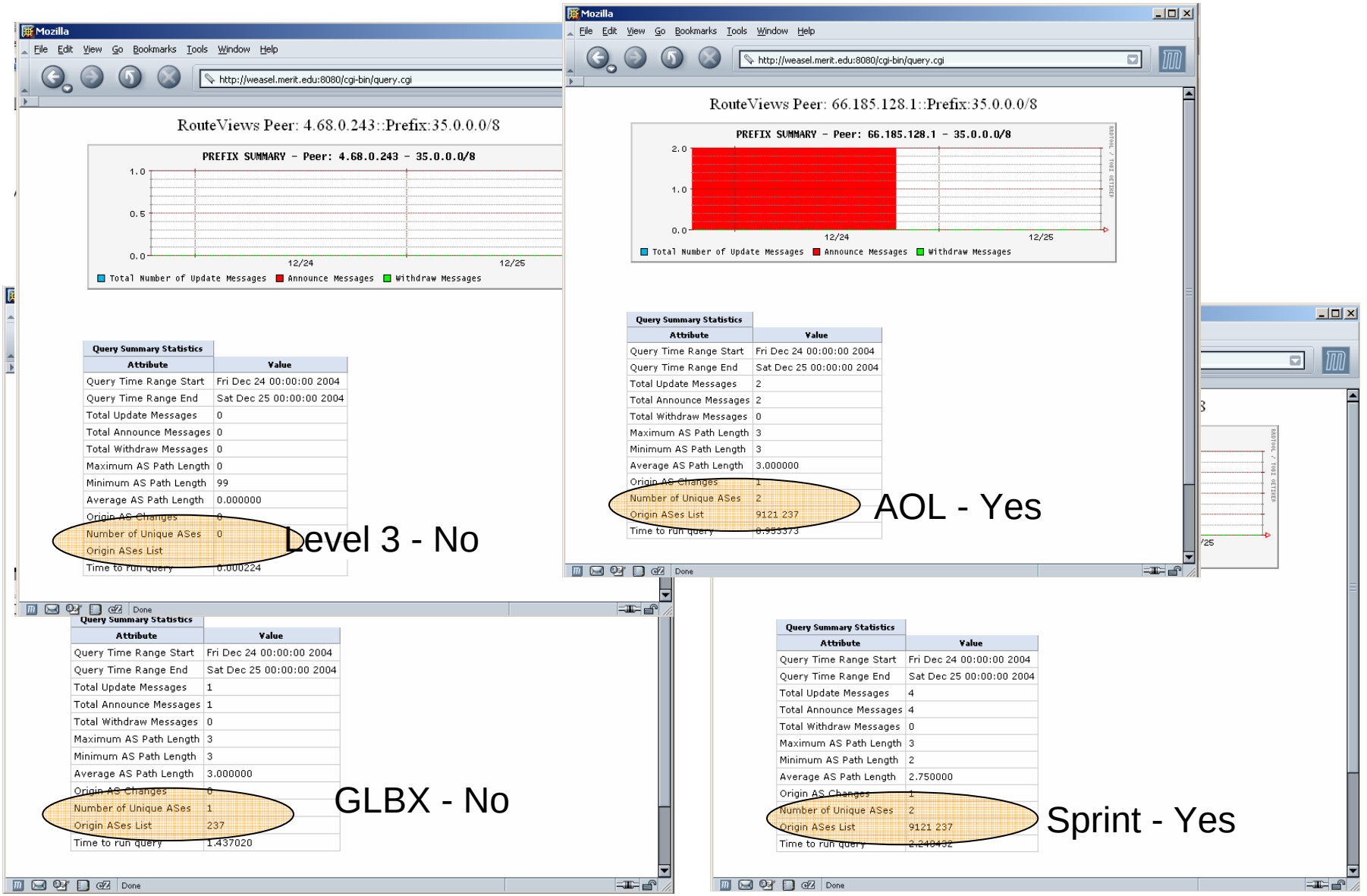


Step 2: Was I affected?/Should I care?

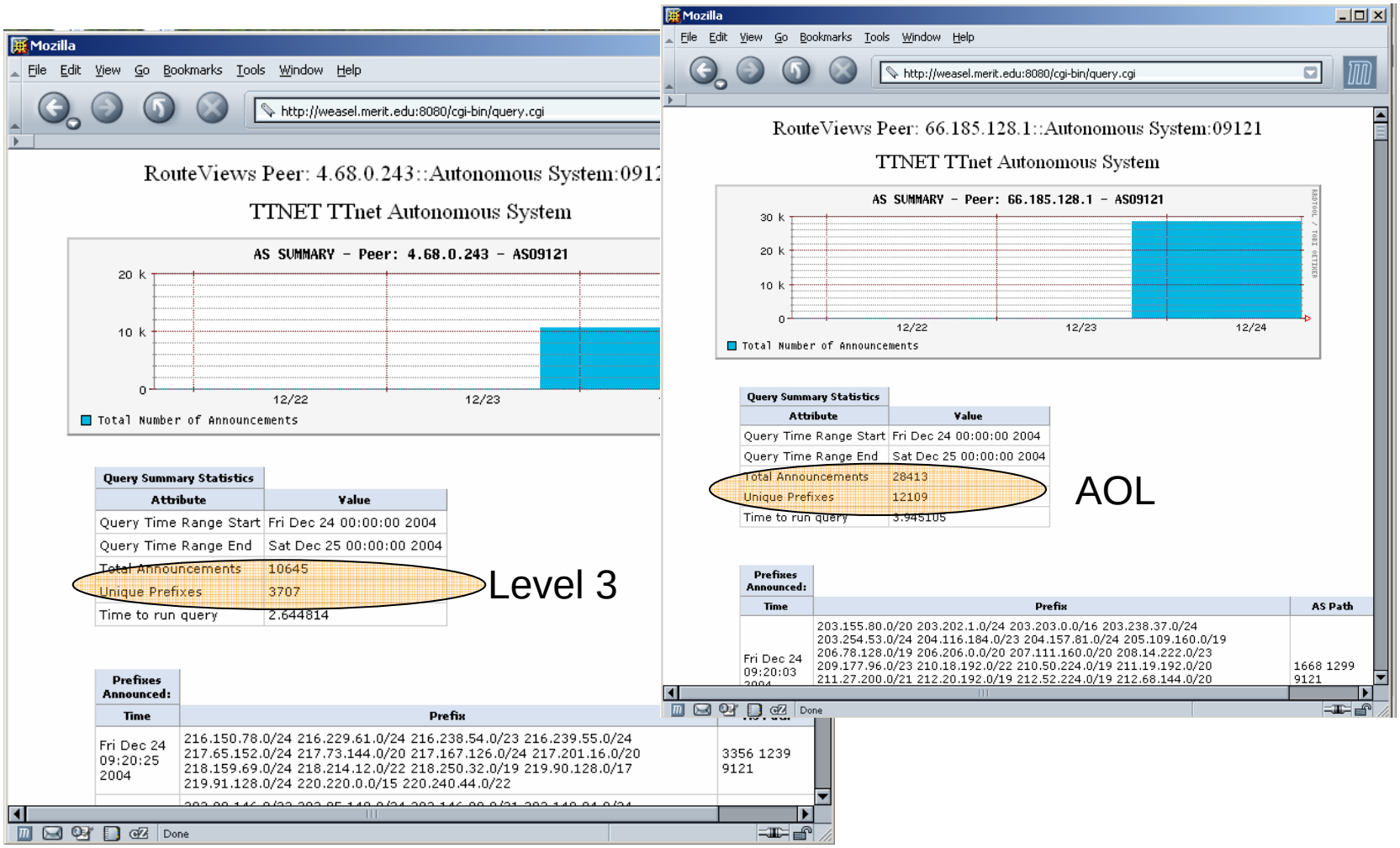




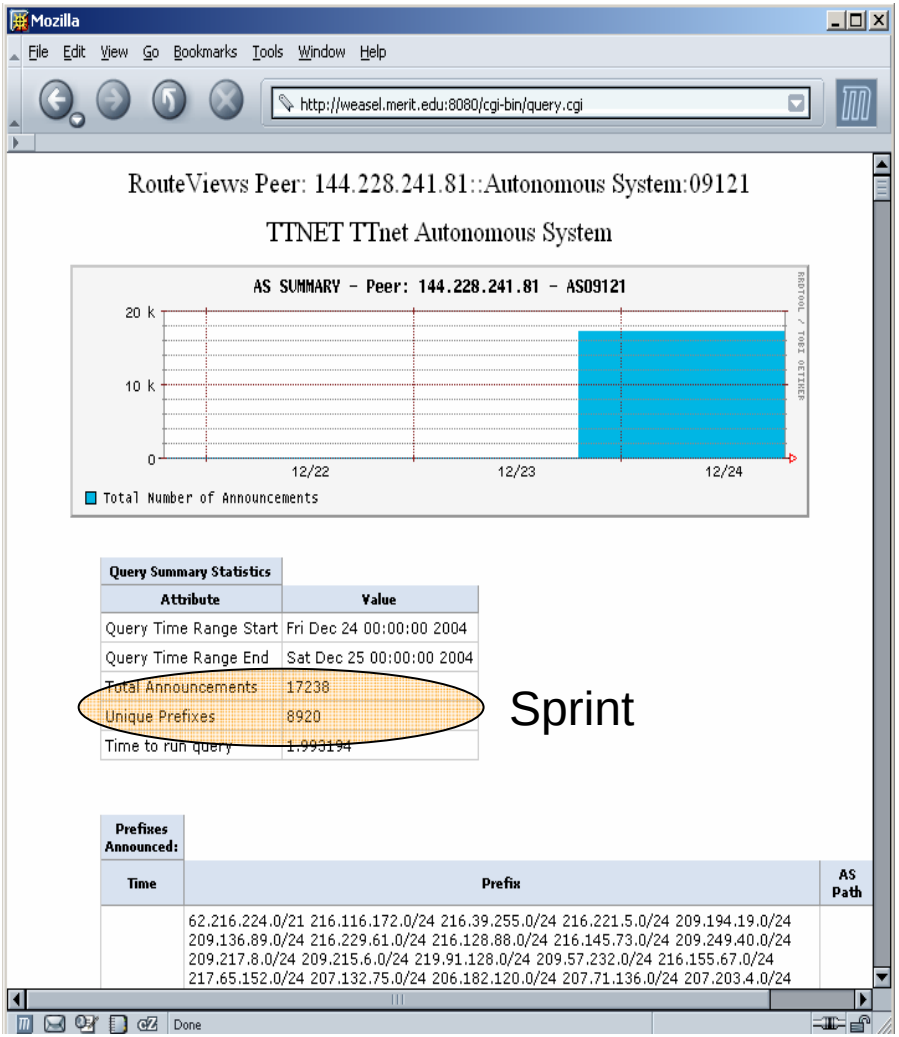
Step 3: Where…

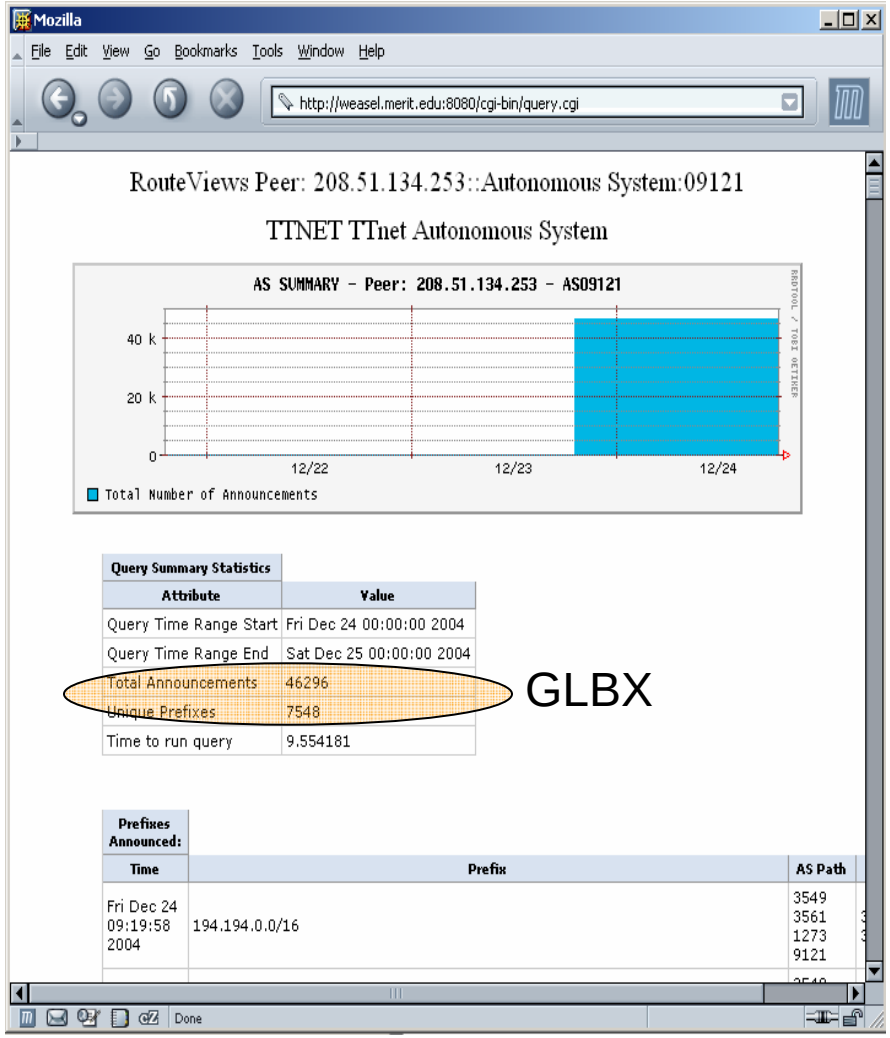

Mozilla
File Edit View Go Bookmarks Tools Window Help
http://weasel.merit.edu:8080/cgi-bin/query.cgi
RouteViews Peer: 4.68.0.243::Prefix:35.0.0.0/8
PREFIX SUMMARY - Peer: 4.68.0.243 - 35.0.0.0/8
1.0
0.5
0.0
12/24
12/25
Total Number of Update Messages
Announce Messages
Withdraw Messages
Query Summary Statistics
Attribute
Value
Query Time Range Start
Fri Dec 24 00:00:00 2004
Query Time Range End
Sat Dec 25 00:00:00 2004
Total Update Messages
0
Total Announce Messages
0
Total Withdraw Messages
0
Maximum AS Path Length
0
Minimum AS Path Length
99
Average AS Path Length
0.000000
Origin AS Changes
0
Number of Unique ASes
0
Origin ASes List
Time to run query
0.000224
Level 3 - No
Mozilla
File Edit View Go Bookmarks Tools Window Help
http://weasel.merit.edu:8080/cgi-bin/query.cgi
RouteViews Peer: 66.185.128.1::Prefix:35.0.0.0/8
PREFIX SUMMARY - Peer: 66.185.128.1 - 35.0.0.0/8
2.0
1.0
0.0
12/24
12/25
Total Number of Update Messages
Announce Messages
Withdraw Messages
Query Summary Statistics
Attribute
Value
Query Time Range Start
Fri Dec 24 00:00:00 2004
Query Time Range End
Sat Dec 25 00:00:00 2004
Total Update Messages
2
Total Announce Messages
2
Total Withdraw Messages
0
Maximum AS Path Length
3
Minimum AS Path Length
3
Average AS Path Length
3.000000
Origin AS Changes
1
Number of Unique ASes
2
Origin ASes List
9121 237
Time to run query
0.953373
AOL - Yes
Done
Query Summary Statistics
Attribute
Value
Query Time Range Start
Fri Dec 24 00:00:00 2004
Query Time Range End
Sat Dec 25 00:00:00 2004
Total Update Messages
1
Total Announce Messages
1
Total Withdraw Messages
0
Maximum AS Path Length
3
Minimum AS Path Length
3
Average AS Path Length
3.000000
Origin AS Changes
0
Number of Unique ASes
1
Origin ASes List
237
Time to run query
1.437020
GLBX - No
Done
Query Summary Statistics
Attribute
Value
Query Time Range Start
Fri Dec 24 00:00:00 2004
Query Time Range End
Sat Dec 25 00:00:00 2004
Total Update Messages
4
Total Announce Messages
4
Total Withdraw Messages
0
Maximum AS Path Length
3
Minimum AS Path Length
2
Average AS Path Length
2.750000
Origin AS Changes
1
Number of Unique ASes
2
Origin ASes List
9121 237
Time to run query
2.240432
Sprint - Yes
Done

Step 4: How widespread…

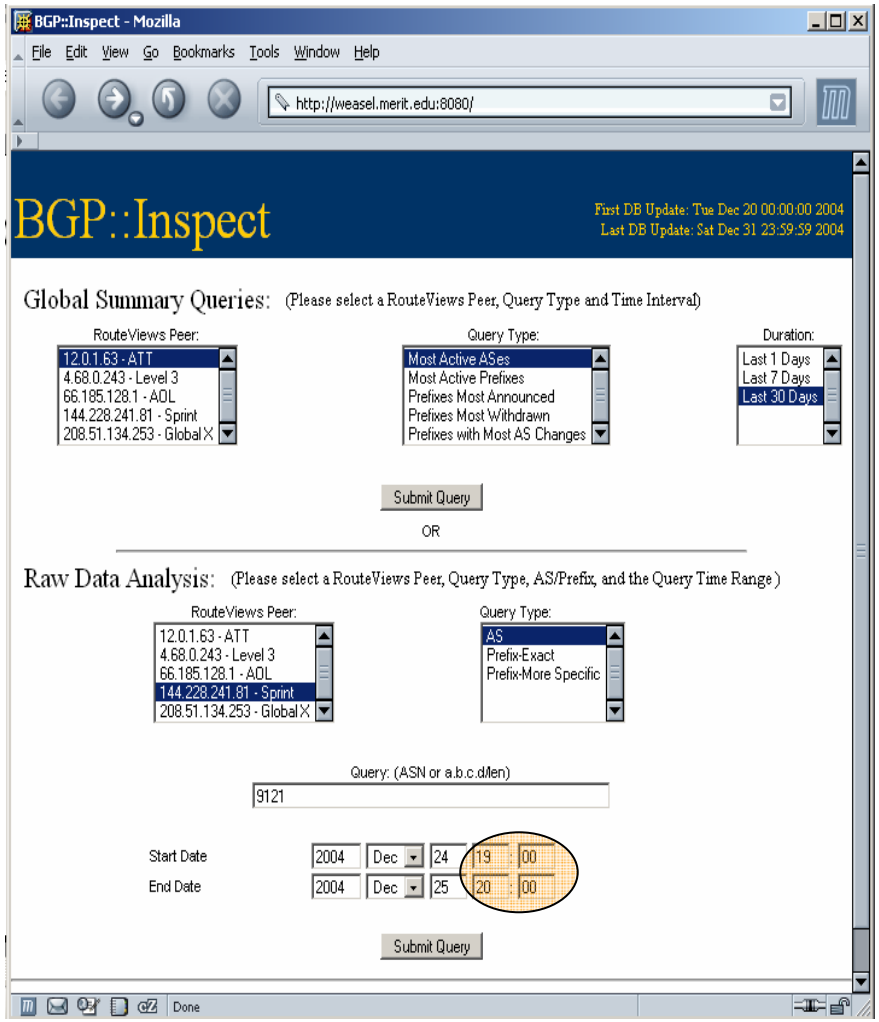


Step 4: How widespread…





Step 5: How long…



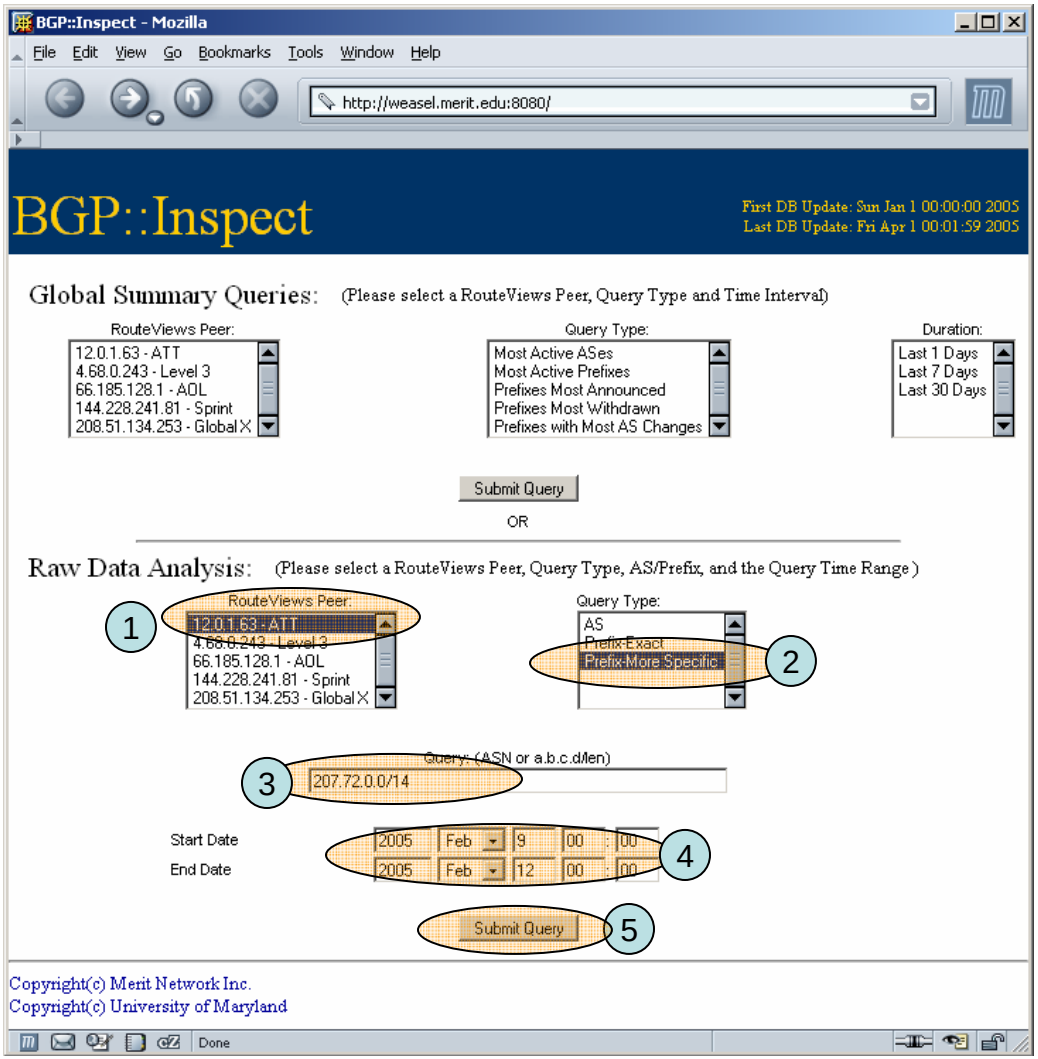
Time	Unique Prefixes Announced by 9121 as seen by Sprint
07-08	0
08-09	0
09-10	**4604**
10-11	56
11-12	804
12-13	56
13-14	196
14-15	159
15-16	34
16-17	92
17-18	54
18-19	172
19-20	**4496**
20-21	229
21-22	15
22-23	0

Primary Event

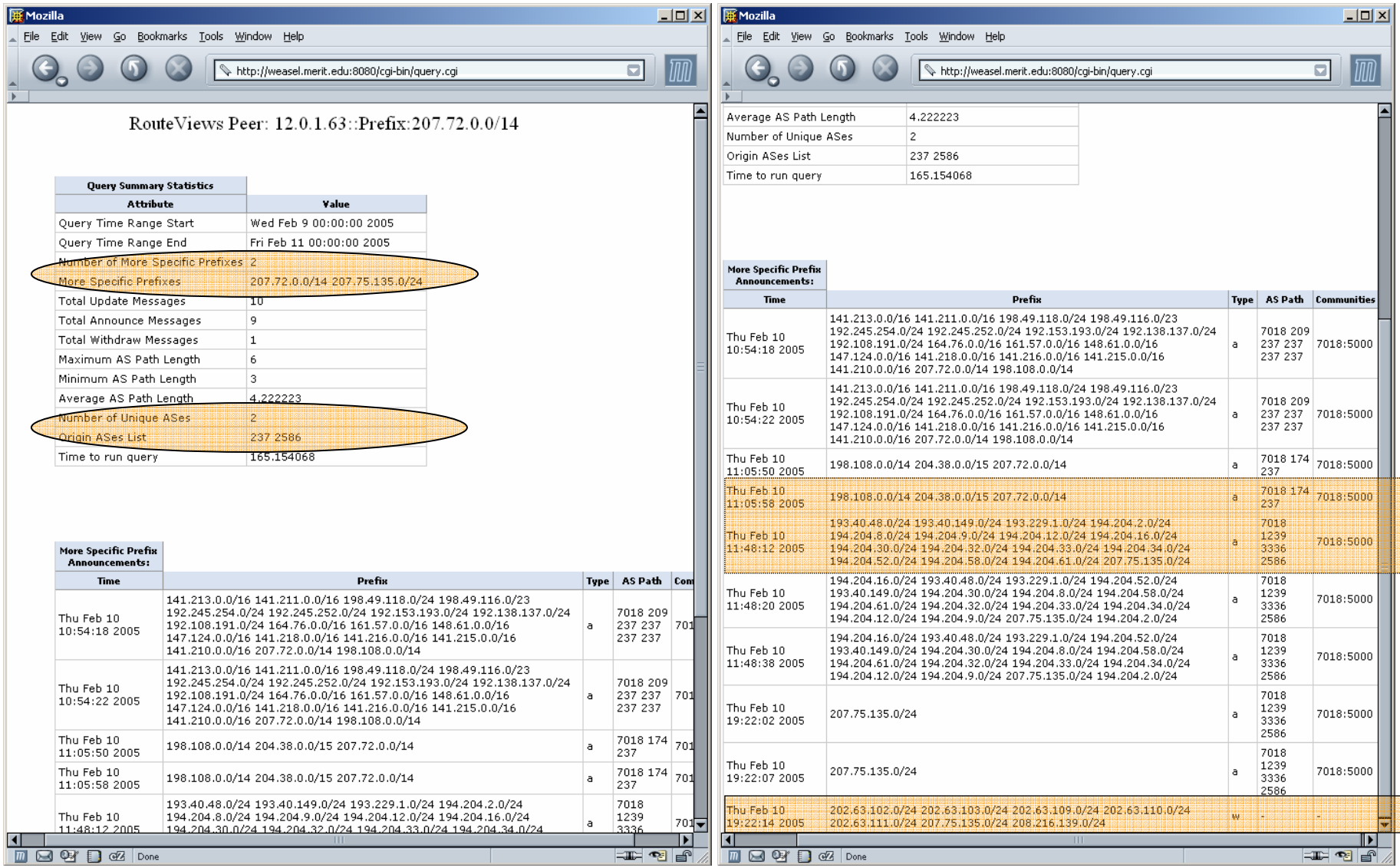
Secondary Event

Case Study 2 – Prefix Hijack Incident

- Incident: On Feb 10th, AS2586, announces 207.75.135.0/24, which is part of Merit's CIDR block 207.72.0.0/14
- Trouble ticket filed, bogus announcement withdrawn by AS2586 by Feb 10th, 19:22hrs
- How do we find out what happened?
- Could there have been automated detection?
- What was the impact, how widespread was it?



Step 1 – Finding out what happened…



Mozilla

File Edit View Go Bookmarks Tools Window Help

http://weasel.merit.edu:8080/cgi-bin/query.cgi

RouteViews Peer: 12.0.1.63::Prefix:207.72.0.0/14

Query Summary Statistics	
Attribute	**Value**
Query Time Range Start	Wed Feb 9 00:00:00 2005
Query Time Range End	Fri Feb 11 00:00:00 2005
Number of More Specific Prefixes	2
More Specific Prefixes	207.72.0.0/14 207.75.135.0/24
Total Update Messages	10
Total Announce Messages	9
Total Withdraw Messages	1
Maximum AS Path Length	6
Minimum AS Path Length	3
Average AS Path Length	4.222223
Number of Unique ASes	2
Origin ASes List	237 2586
Time to run query	165.154068

More Specific Prefix Announcements:

Time	Prefix	Type	AS Path	Com
Thu Feb 10 10:54:18 2005	141.213.0.0/16 141.211.0.0/16 198.49.118.0/24 198.49.116.0/23 192.245.254.0/24 192.245.252.0/24 192.153.193.0/24 192.138.137.0/24 192.108.191.0/24 164.76.0.0/16 161.57.0.0/16 148.61.0.0/16 147.124.0.0/16 141.218.0.0/16 141.216.0.0/16 141.215.0.0/16 141.210.0.0/16 207.72.0.0/14 198.108.0.0/14	a	7018 209 237 237 237 237	701
Thu Feb 10 10:54:22 2005	141.213.0.0/16 141.211.0.0/16 198.49.118.0/24 198.49.116.0/23 192.245.254.0/24 192.245.252.0/24 192.153.193.0/24 192.138.137.0/24 192.108.191.0/24 164.76.0.0/16 161.57.0.0/16 148.61.0.0/16 147.124.0.0/16 141.218.0.0/16 141.216.0.0/16 141.215.0.0/16 141.210.0.0/16 207.72.0.0/14 198.108.0.0/14	a	7018 209 237 237 237 237	701
Thu Feb 10 11:05:50 2005	198.108.0.0/14 204.38.0.0/15 207.72.0.0/14	a	7018 174 237	701
Thu Feb 10 11:05:58 2005	198.108.0.0/14 204.38.0.0/15 207.72.0.0/14	a	7018 174 237	701
Thu Feb 10 11:48:12 2005	193.40.48.0/24 193.40.149.0/24 193.229.1.0/24 194.204.2.0/24 194.204.8.0/24 194.204.9.0/24 194.204.12.0/24 194.204.16.0/24 194.204.30.0/24 194.204.32.0/24 194.204.33.0/24 194.204.34.0/24	a	7018 1239 3336	701

Mozilla

File Edit View Go Bookmarks Tools Window Help

http://weasel.merit.edu:8080/cgi-bin/query.cgi

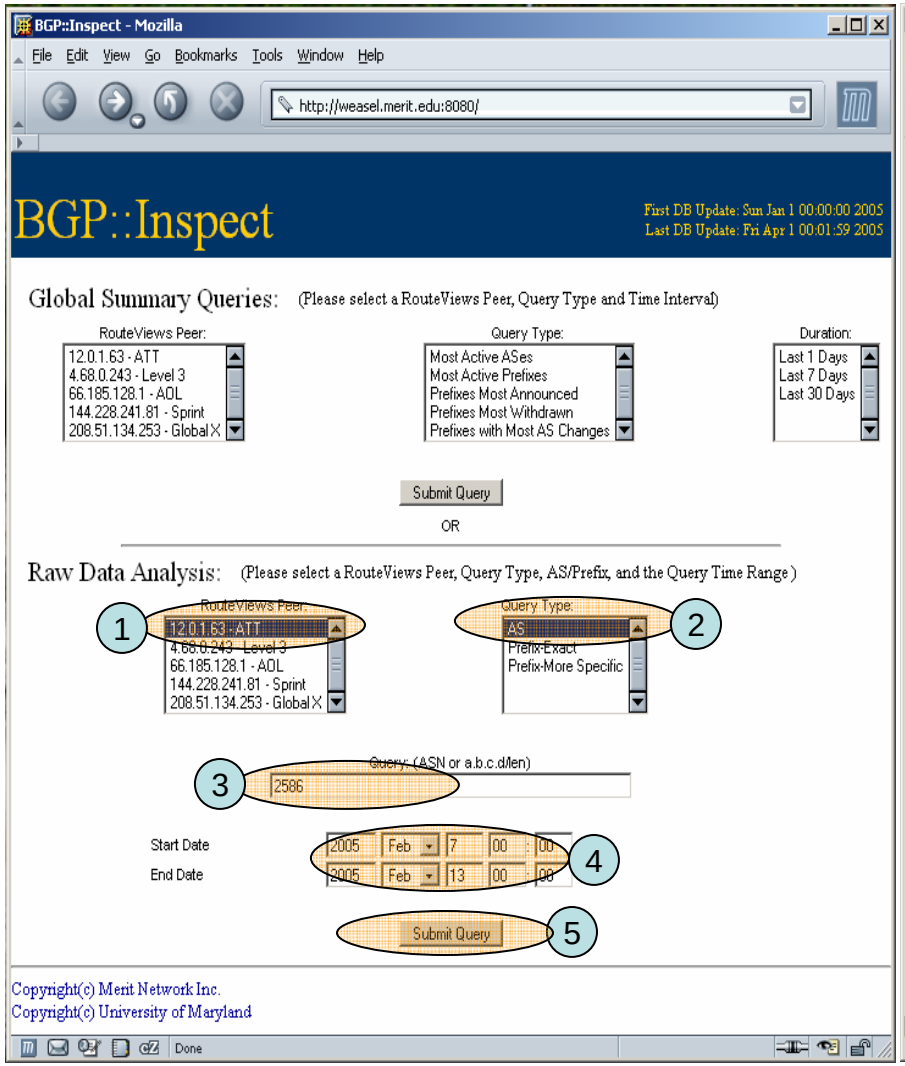
Average AS Path Length	4.222223
Number of Unique ASes	2
Origin ASes List	237 2586
Time to run query	165.154068

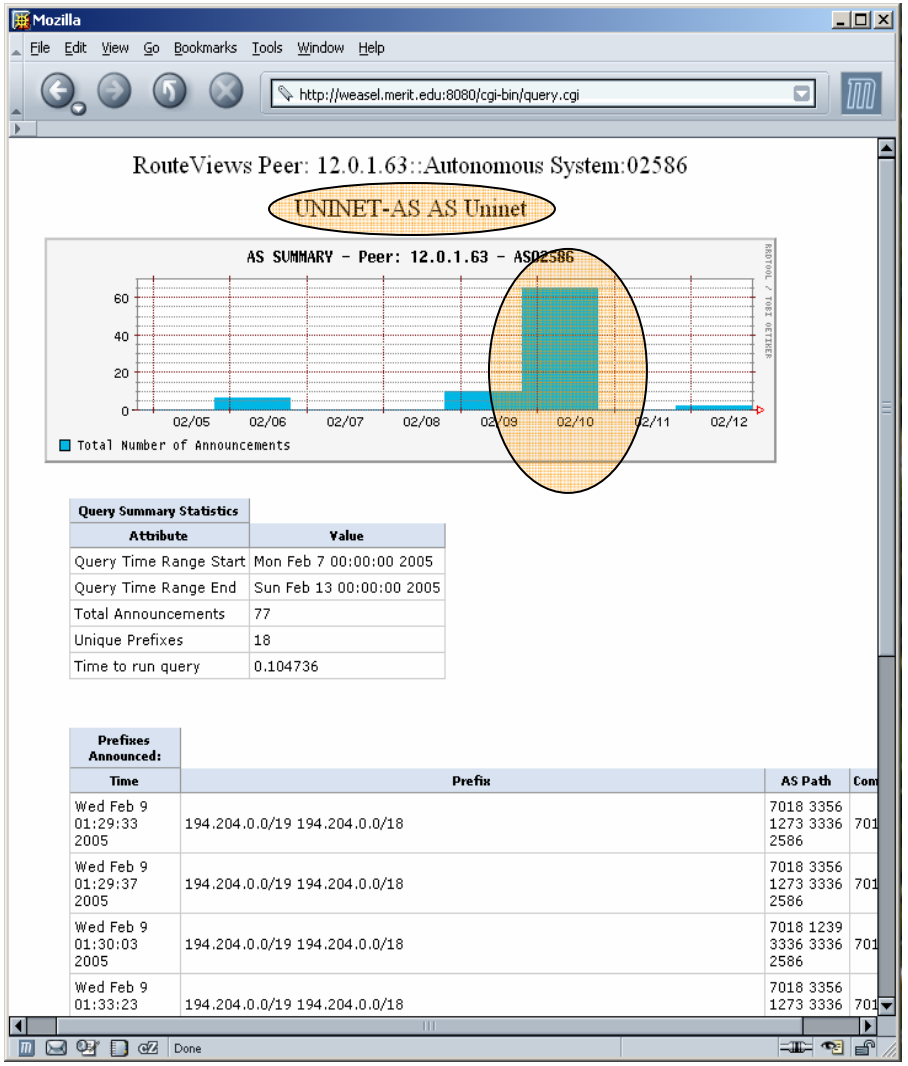
More Specific Prefix Announcements:

Time	Prefix	Type	AS Path	Communities
Thu Feb 10 10:54:18 2005	141.213.0.0/16 141.211.0.0/16 198.49.118.0/24 198.49.116.0/23 192.245.254.0/24 192.245.252.0/24 192.153.193.0/24 192.138.137.0/24 192.108.191.0/24 164.76.0.0/16 161.57.0.0/16 148.61.0.0/16 147.124.0.0/16 141.218.0.0/16 141.216.0.0/16 141.215.0.0/16 141.210.0.0/16 207.72.0.0/14 198.108.0.0/14	a	7018 209 237 237 237 237	7018:5000
Thu Feb 10 10:54:22 2005	141.213.0.0/16 141.211.0.0/16 198.49.118.0/24 198.49.116.0/23 192.245.254.0/24 192.245.252.0/24 192.153.193.0/24 192.138.137.0/24 192.108.191.0/24 164.76.0.0/16 161.57.0.0/16 148.61.0.0/16 147.124.0.0/16 141.218.0.0/16 141.216.0.0/16 141.215.0.0/16 141.210.0.0/16 207.72.0.0/14 198.108.0.0/14	a	7018 209 237 237 237 237	7018:5000
Thu Feb 10 11:05:50 2005	198.108.0.0/14 204.38.0.0/15 207.72.0.0/14	a	7018 174 237	7018:5000
Thu Feb 10 11:05:58 2005	198.108.0.0/14 204.38.0.0/15 207.72.0.0/14	a	7018 174 237	7018:5000
Thu Feb 10 11:48:12 2005	193.40.48.0/24 193.40.149.0/24 193.229.1.0/24 194.204.2.0/24 194.204.8.0/24 194.204.9.0/24 194.204.12.0/24 194.204.16.0/24 194.204.30.0/24 194.204.32.0/24 194.204.33.0/24 194.204.34.0/24 194.204.52.0/24 194.204.58.0/24 194.204.61.0/24 207.75.135.0/24	a	7018 1239 3336 2586	7018:5000
Thu Feb 10 11:48:20 2005	194.204.16.0/24 193.40.48.0/24 193.229.1.0/24 194.204.52.0/24 193.40.149.0/24 194.204.30.0/24 194.204.8.0/24 194.204.58.0/24 194.204.61.0/24 194.204.32.0/24 194.204.33.0/24 194.204.34.0/24 194.204.12.0/24 194.204.9.0/24 207.75.135.0/24 194.204.2.0/24	a	7018 1239 3336 2586	7018:5000
Thu Feb 10 11:48:38 2005	194.204.16.0/24 193.40.48.0/24 193.229.1.0/24 194.204.52.0/24 193.40.149.0/24 194.204.30.0/24 194.204.8.0/24 194.204.58.0/24 194.204.61.0/24 194.204.32.0/24 194.204.33.0/24 194.204.34.0/24 194.204.12.0/24 194.204.9.0/24 207.75.135.0/24 194.204.2.0/24	a	7018 1239 3336 2586	7018:5000
Thu Feb 10 19:22:02 2005	207.75.135.0/24	a	7018 1239 3336 2586	7018:5000
Thu Feb 10 19:22:07 2005	207.75.135.0/24	a	7018 1239 3336 2586	7018:5000
Thu Feb 10 19:22:14 2005	202.63.102.0/24 202.63.103.0/24 202.63.109.0/24 202.63.110.0/24 202.63.111.0/24 207.75.135.0/24 208.216.139.0/24	w	-	-

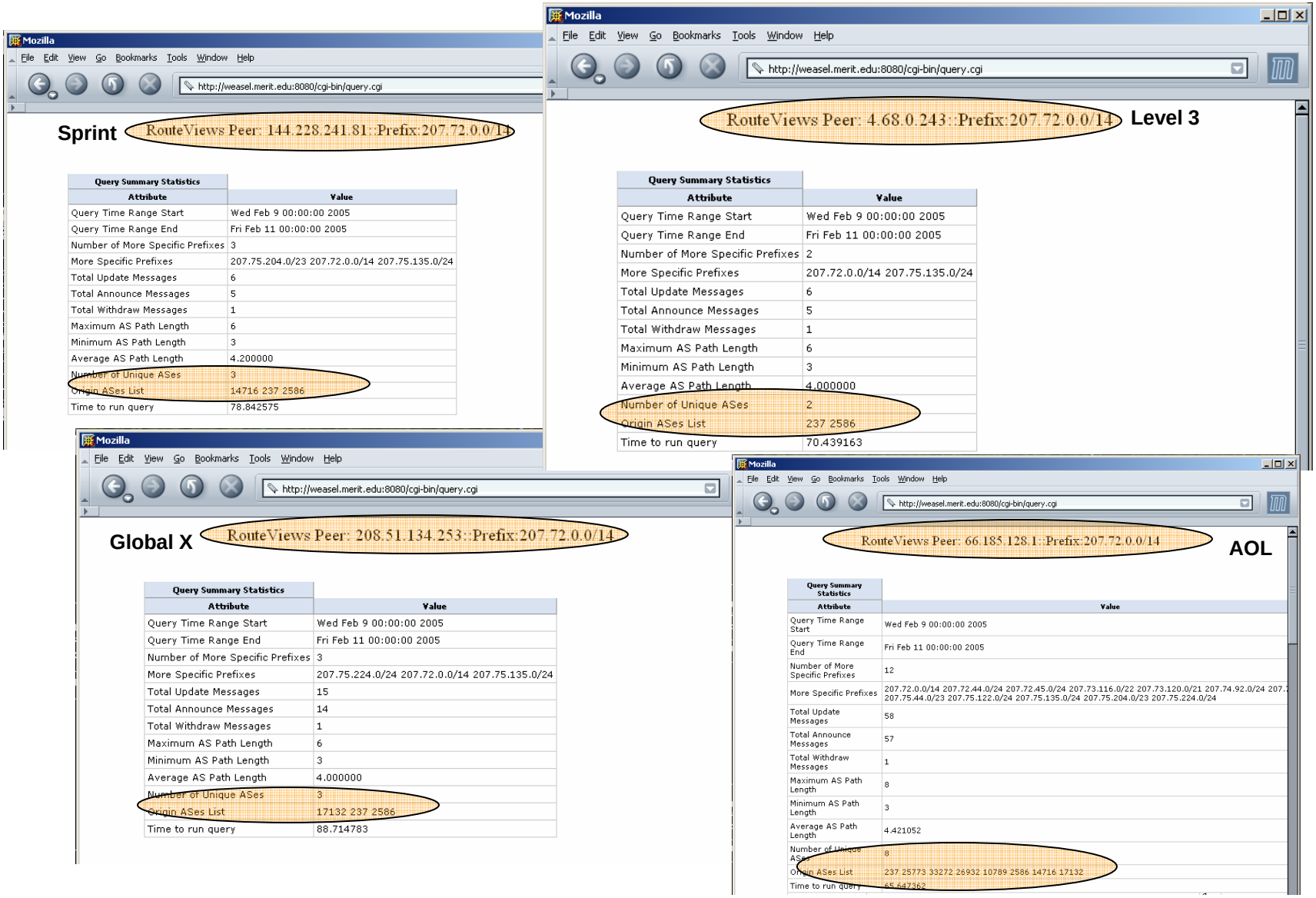
Done

Step 2 – Who, why…





Step 3 – where…


Mozilla
File Edit View Go Bookmarks Tools Window Help
http://weasel.merit.edu:8080/cgi-bin/query.cgi
Sprint
RouteViews Peer: 144.228.241.81::Prefix:207.72.0.0/14
Query Summary Statistics
Attribute | Value
Query Time Range Start | Wed Feb 9 00:00:00 2005
Query Time Range End | Fri Feb 11 00:00:00 2005
Number of More Specific Prefixes | 3
More Specific Prefixes | 207.75.204.0/23 207.72.0.0/14 207.75.135.0/24
Total Update Messages | 6
Total Announce Messages | 5
Total Withdraw Messages | 1
Maximum AS Path Length | 6
Minimum AS Path Length | 3
Average AS Path Length | 4.200000
Number of Unique ASes | 3
Origin ASes List | 14716 237 2586
Time to run query | 78.842575
Mozilla
File Edit View Go Bookmarks Tools Window Help
http://weasel.merit.edu:8080/cgi-bin/query.cgi
RouteViews Peer: 4.68.0.243::Prefix:207.72.0.0/14
Level 3
Query Summary Statistics
Attribute | Value
Query Time Range Start | Wed Feb 9 00:00:00 2005
Query Time Range End | Fri Feb 11 00:00:00 2005
Number of More Specific Prefixes | 2
More Specific Prefixes | 207.72.0.0/14 207.75.135.0/24
Total Update Messages | 6
Total Announce Messages | 5
Total Withdraw Messages | 1
Maximum AS Path Length | 6
Minimum AS Path Length | 3
Average AS Path Length | 4.000000
Number of Unique ASes | 2
Origin ASes List | 237 2586
Time to run query | 70.439163
Mozilla
File Edit View Go Bookmarks Tools Window Help
http://weasel.merit.edu:8080/cgi-bin/query.cgi
Global X
RouteViews Peer: 208.51.134.253::Prefix:207.72.0.0/14
Query Summary Statistics
Attribute | Value
Query Time Range Start | Wed Feb 9 00:00:00 2005
Query Time Range End | Fri Feb 11 00:00:00 2005
Number of More Specific Prefixes | 3
More Specific Prefixes | 207.75.224.0/24 207.72.0.0/14 207.75.135.0/24
Total Update Messages | 15
Total Announce Messages | 14
Total Withdraw Messages | 1
Maximum AS Path Length | 6
Minimum AS Path Length | 3
Average AS Path Length | 4.000000
Number of Unique ASes | 3
Origin ASes List | 17132 237 2586
Time to run query | 88.714783
Mozilla
File Edit View Go Bookmarks Tools Window Help
http://weasel.merit.edu:8080/cgi-bin/query.cgi
RouteViews Peer: 66.185.128.1::Prefix:207.72.0.0/14
AOL
Query Summary Statistics
Attribute | Value
Query Time Range Start | Wed Feb 9 00:00:00 2005
Query Time Range End | Fri Feb 11 00:00:00 2005
Number of More Specific Prefixes | 12
More Specific Prefixes | 207.72.0.0/14 207.72.44.0/24 207.72.45.0/24 207.73.116.0/22 207.73.120.0/21 207.74.92.0/24 207.75.44.0/23 207.75.122.0/24 207.75.135.0/24 207.75.204.0/23 207.75.224.0/24
Total Update Messages | 58
Total Announce Messages | 57
Total Withdraw Messages | 1
Maximum AS Path Length | 8
Minimum AS Path Length | 3
Average AS Path Length | 4.421052
Number of Unique ASes | 8
Origin ASes List | 237 25773 33272 26932 10789 2586 14716 17132
Time to run query | 65.647362

Conclusions and Future Work

- There is a need to build efficient tools that help extract useful information from large BGP datasets
- BGP::Inspect is currently available to the network operator and research communities and feedback is appreciated
- Aside from BGP::Inspect we have presented some basic techniques such as chunked-compressed files, B+ Tree indexing, data redundancy elimination, and caching that can be applied by other data mining tools to help analyze other large datasets as well.
- The goal is not just to provide access to the data, but to try to provider useful data summaries as well, that can help researchers and network operators quickly identify potentially “interesting” events. Top20 lists are a good way to bring potentially interesting things to the attention of people.
- Tools need to be useful before they can be used, and in order to be useful, feedback from potential users is critical.
- BGP data analysis need not be hard/painful/tedious, that’s what tools are for!
- Where do we go from here, so we have basic capabilities what about:
  - Automated anomaly detection, notification, same tool?, different tool?
  - More scalability,? What are the limits?
  - What are more useful queries? What book-keeping do we need to track those?