DEFCON 16:

How to evade geospatial intrusion detection techniques

Ryan W. Trost

Agenda

- GIS
- Geospatial Intrusion Detection implementations
- Geospatial Intrusion Detection methodology
- Accuracy of IP -> lat/long translation
- Okay…so how do I beat it?
- Q&A

GIS

- GIS (Geographic Information Systems): computer based methodology to collect, store, manipulate, retrieve, display and analyze georeferenced data.
  - GoogleEarth
  - ESRI
  - Intergraph
  - GRASS

GIS

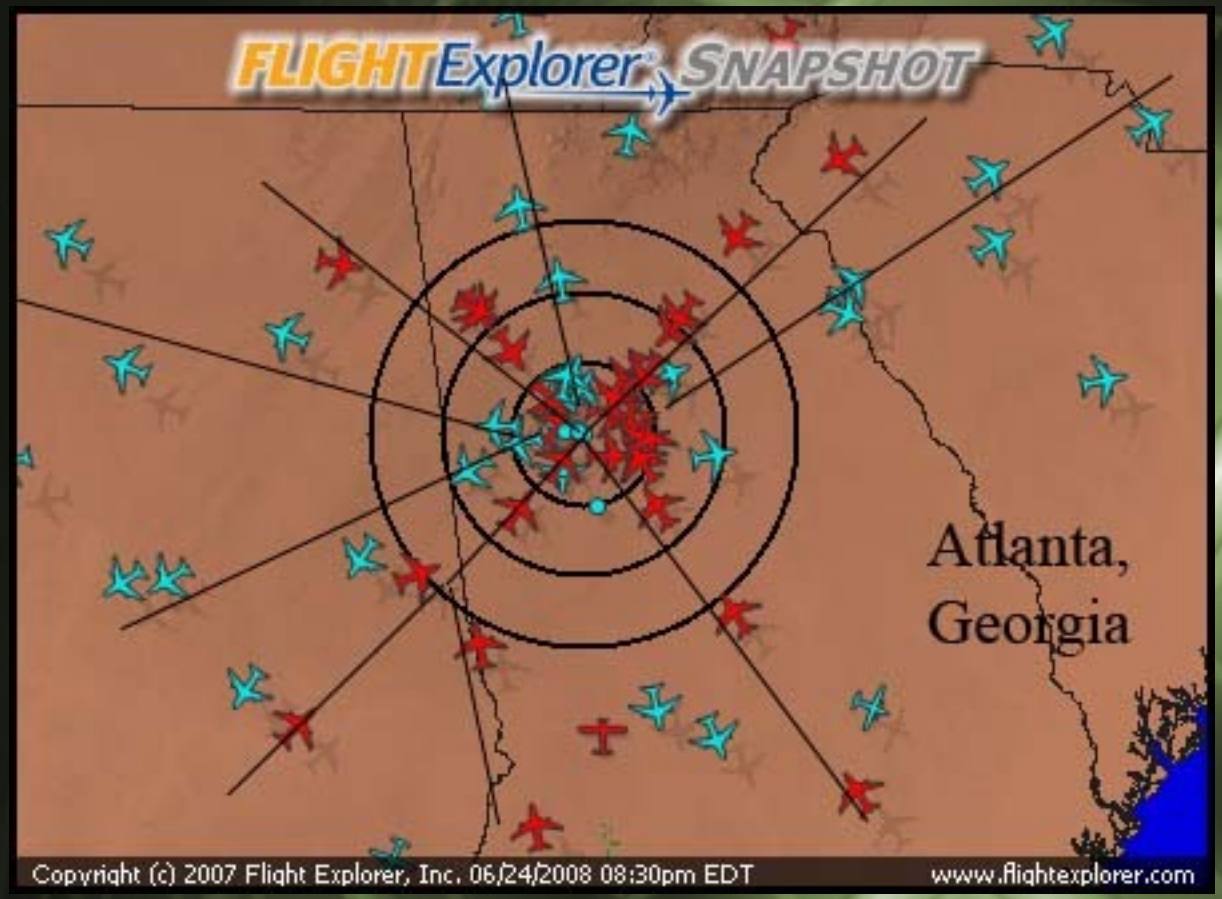
- Traditional GIS tools focused more on environmental issues
- These days thanks to GoogleEarth and/or GoogleMaps the average Internet user is starting to be exposed to the power that mapping software unleashes.
  - Track a cell phone (cell tower triangulation)
  - Track flights in mid-air!!!

Cell Phone


ethantw1219
@ 3d 14h 39m ago
7th Ave
Exit
Prefs


MOLOGOGO
Home Locations Friends Downloads Account Logout
Logged in as ethantw1220
Spotted ethantw1219
@ 01:33 PM CST on 02/17/2006
Add this spot as a Saved Location
View last 100 points from ethantw1219
Tags:
Last message to you:
Send a message to ethantw1219
Privacy Policy & Terms | Email Us | About | Blog | Wiki | Mailing Lists | Phone Sales

Track Any Flight



Where has IT security and mapping collided?

- Multiple security firms have implemented GIS tools in their products (in varying degrees)
  - MeerCat (Secure Decisions)
  - VisCat (ETRI)
  - GeoSWAT

MeerCat

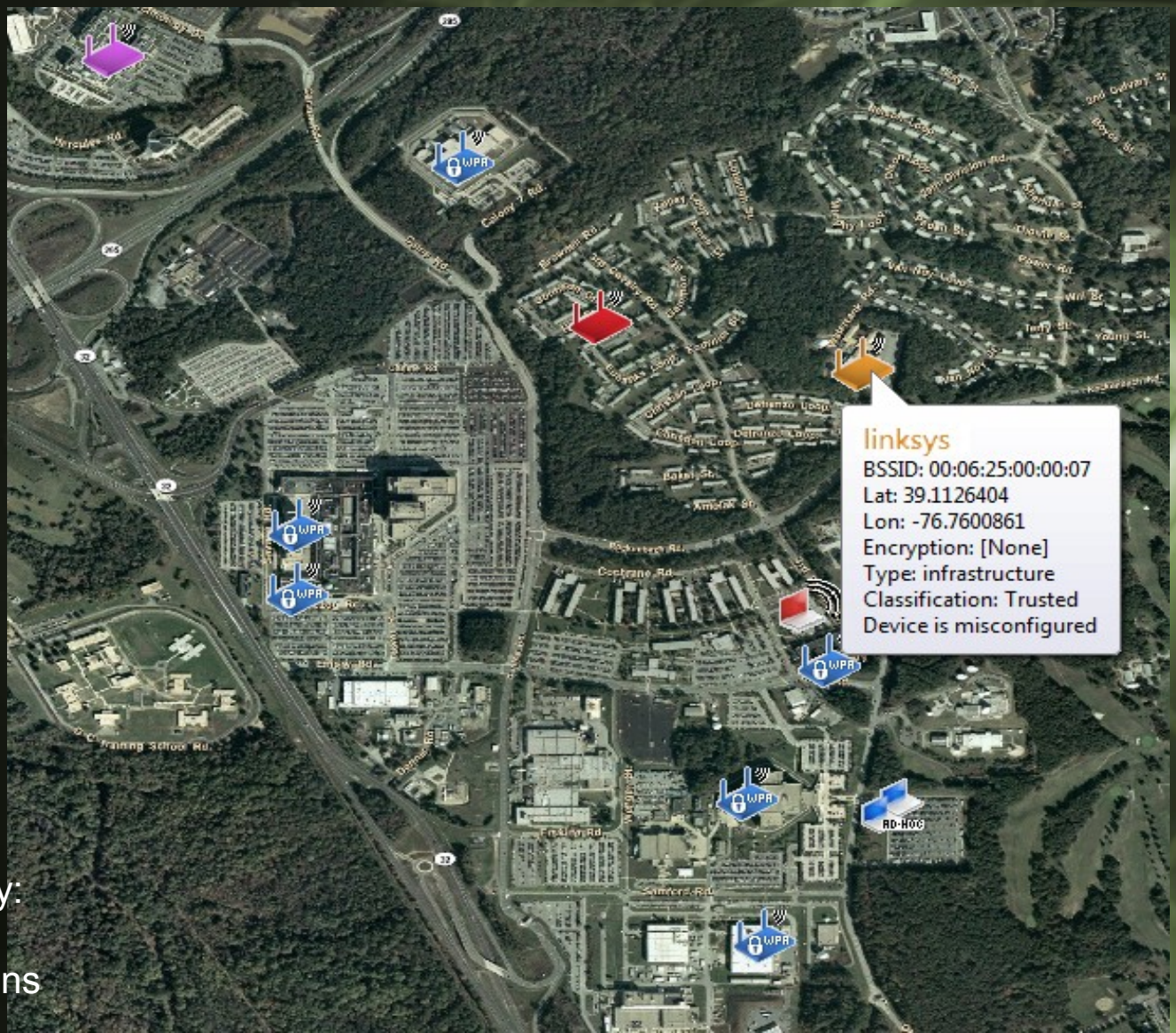
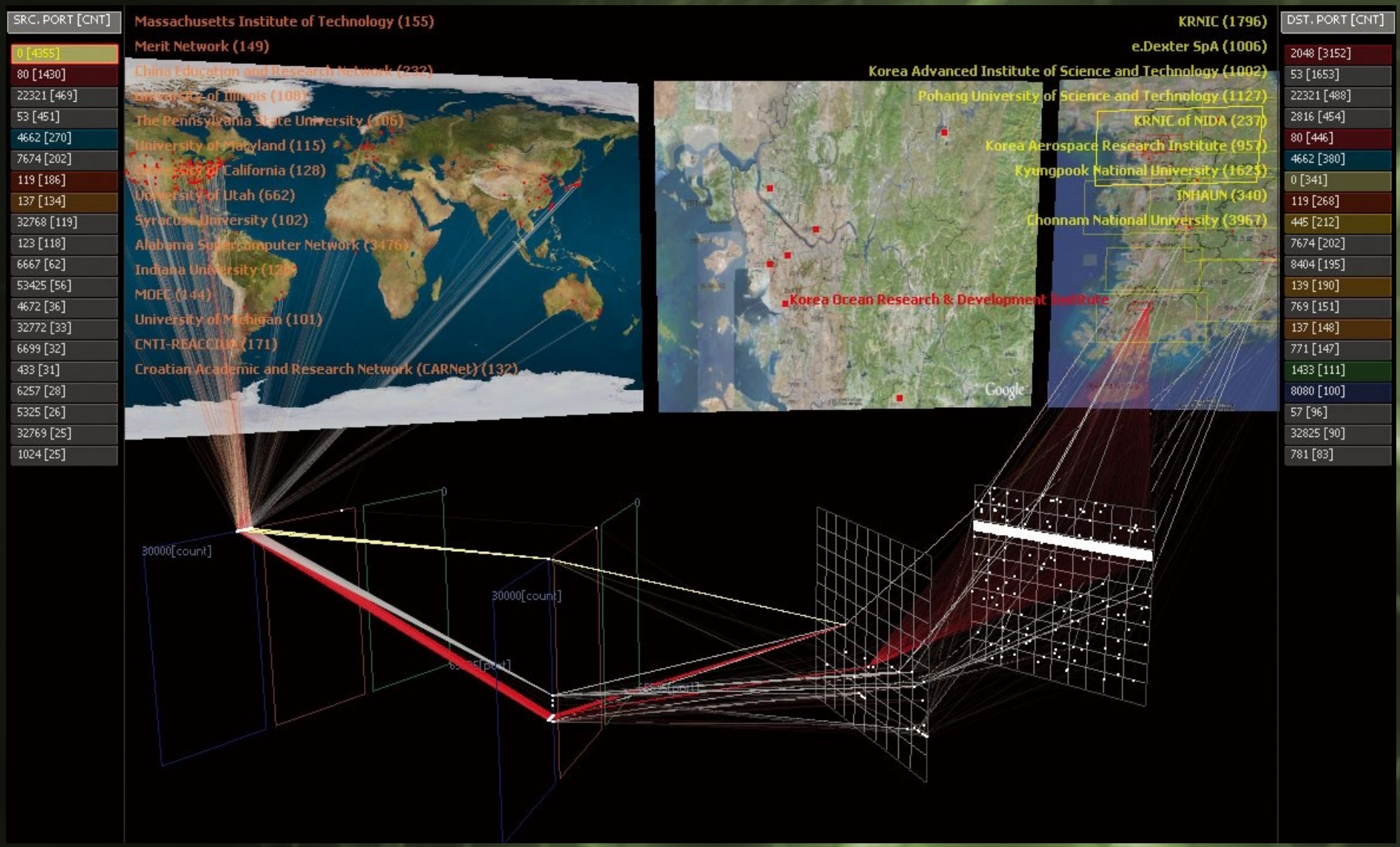
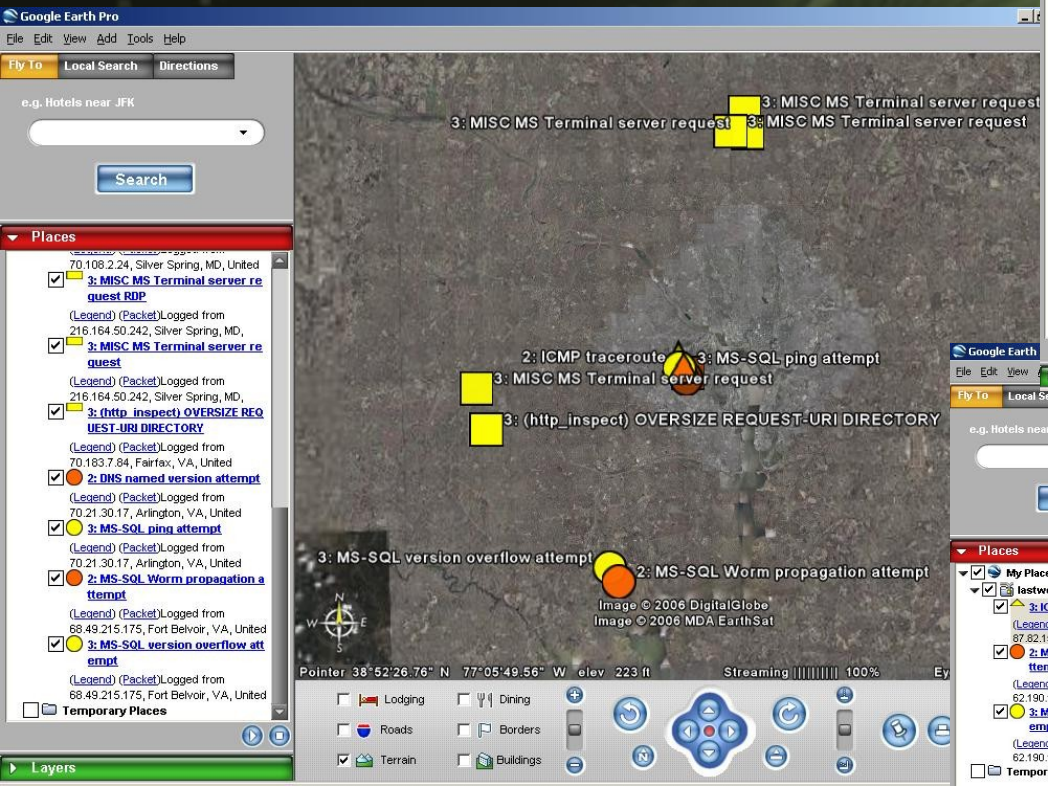


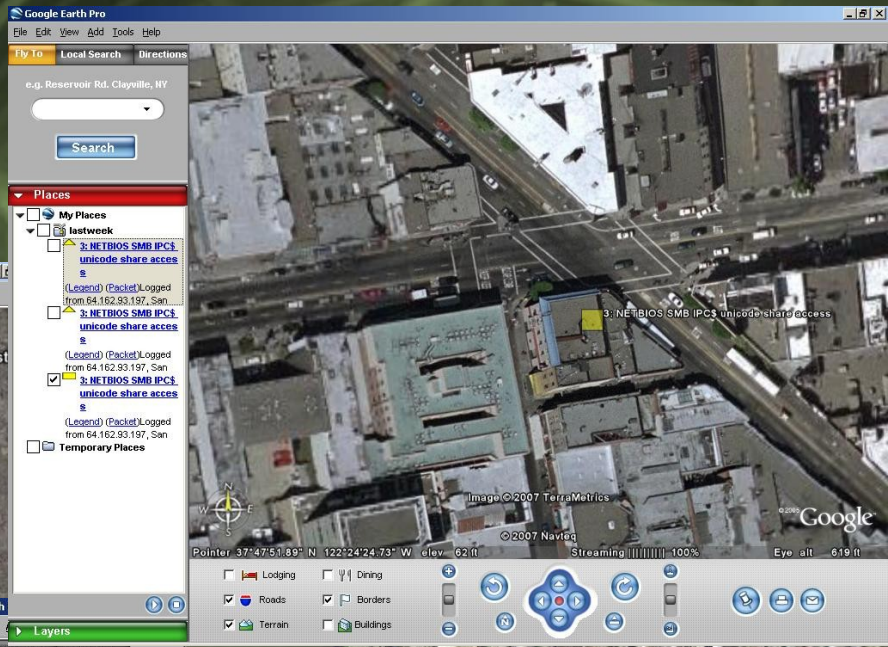
Image Courtesy:
John Goodall
Secure Decisions

VizCat

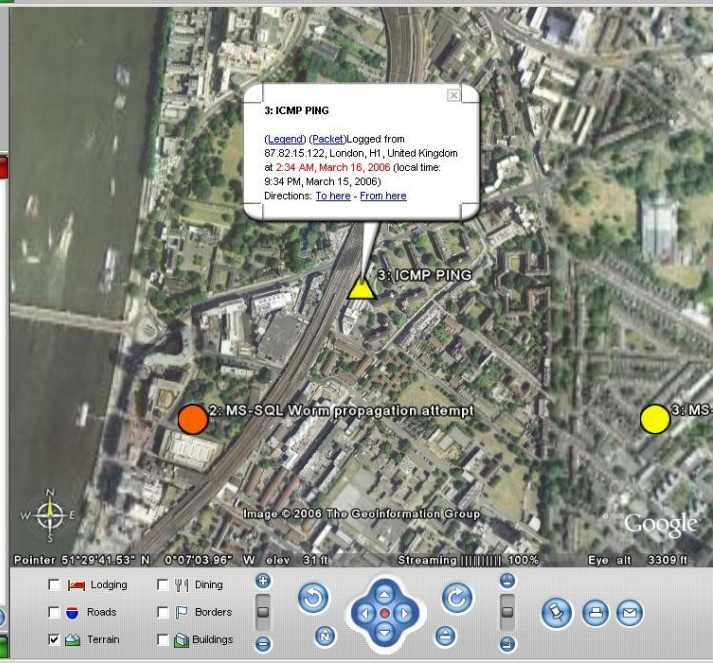

SRC. PORT [CNT]
0 [4355]
80 [1430]
22321 [469]
53 [451]
4662 [270]
7674 [202]
119 [186]
137 [134]
32768 [119]
123 [118]
6667 [62]
53425 [56]
4672 [36]
32772 [33]
6699 [32]
433 [31]
6257 [28]
5325 [26]
32769 [25]
1024 [25]
Massachusetts Institute of Technology (155)
Merit Network (149)
China Education and Research Network (232)
University of Illinois (108)
The Pennsylvania State University (106)
University of Maryland (115)
University of California (128)
University of Utah (662)
Syracuse University (102)
Alabama Supercomputer Network (3476)
Indiana University (128)
MOEC (144)
University of Michigan (101)
CNTI-REACCIUN (171)
Croatian Academic and Research Network (CARNet) (132)
KRNIC (1796)
e.Dexter SpA (1006)
Korea Advanced Institute of Science and Technology (1002)
Pohang University of Science and Technology (1127)
KRNIC of NIDA (237)
Korea Aerospace Research Institute (957)
Kyungpook National University (1625)
INHAUN (340)
Chonnam National University (3967)
Korea Ocean Research & Development Institute
Google
DST. PORT [CNT]
2048 [3152]
53 [1653]
22321 [488]
2816 [454]
80 [446]
4662 [380]
0 [341]
119 [268]
445 [212]
7674 [202]
8404 [195]
139 [190]
769 [151]
137 [148]
771 [147]
1433 [111]
8080 [100]
57 [96]
32825 [90]
781 [83]
30000[count]
30000[count]

GeoSWAT


Google Earth Pro
File Edit View Add Tools Help
Fly To Local Search Directions
e.g. Hotels near JFK
Search
Places
3: MISC MS Terminal server request
3: MISC MS Terminal server request
2: ICMP traceroute
3: MS-SQL ping attempt
3: MISC MS Terminal server request
3: (http_inspect) OVERSIZE REQUEST-URI DIRECTORY
3: MS-SQL version overflow attempt
2: MS-SQL Worm propagation attempt
Image © 2006 DigitalGlobe
Image © 2006 MDA EarthSat
Pointer 38°52'26.76" N 77°05'49.56" W elev 223 ft
Streaming 100%
Lodging Dining
Roads Borders
Terrain Buildings
Layers


Google Earth Pro
File Edit View Add Tools Help
Fly To Local Search Directions
e.g. Reservoir Rd. Clayville, NY
Search
Places
My Places
lastweek
3: NETBIOS SMB IPC$ unicode share access
Temporary Places
3: NETBIOS SMB IPC$ unicode share access
Image © 2007 TerraMetrics
© 2007 Navteq
Google
Pointer 37°47'51.89" N 122°24'24.73" W elev 62 ft
Streaming 100%
Eye alt 619 ft
Lodging Dining
Roads Borders
Terrain Buildings


Google Earth
Fly To Local Search Directions
e.g. Hotels near JFK
Search
Places
My Places
lastweek
3: ICMP PING
2: MS-SQL Worm propagation attempt
3: MS-SQL version overflow attempt
Temporary Places
Layers


3: ICMP PING
(Legend) (Packet)Logged from 87.82.15.122, London, H1, United Kingdom at 2:34 AM, March 16, 2006 (local time: 9:34 PM, March 15, 2006)
Directions: To here - From here
3: ICMP PING
2: MS-SQL Worm propagation attempt
Image © 2006 The GeoInformation Group
Google
Pointer 51°29'41.53" N 0°07'03.96" W elev 31 ft
Streaming 100%
Eye alt 3309 ft
Lodging Dining
Roads Borders
Terrain Buildings

Geospatial Intrusion Detection

- Goal: find a direct correlation between externally based network alerts by plotting their source locations on a geographic map

How does it work?

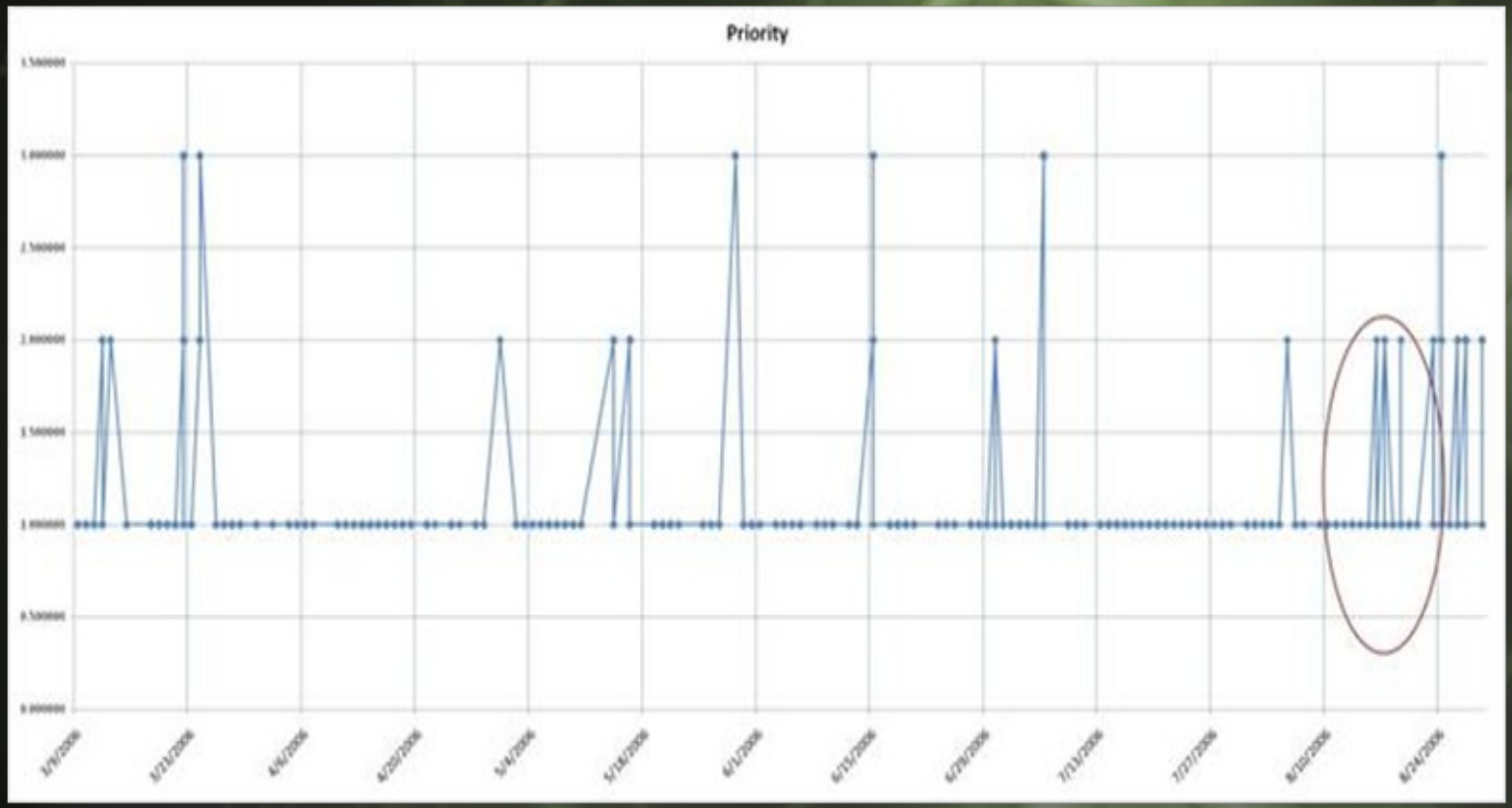
- High-level ‘roadmap’:
  1. Plot rolling time period (1 week/2 weeks/4 weeks)
  2. Eliminate ‘friendlies’ to reduce IDS false positives
     - 2.1 Geographically plot remote branches, SOHO, business partners locations by street address (very accurate in GoogleEarth)
     - 2.2 Create an IDS alert that is triggered when a customer authenticates to a website

Geospatial Intrusion Detection

3. Run a clustering algorithm on plotted data
   - There are several different clustering algorithms to choose from:
     - Poisson, nearest-neighbor, Moran's I Index, Ripley's K Function, Getis-Ord
4. Extract network alerts within identified 'hot-spot'
5. Run a weight calculating algorithm to evaluate if there is a relationship between alerts
   - Correlating elements in an alert
     - Alert severity
     - Destination ports
     - Timestamp

1. Plot rolling timeseries

14 day intervals (the slow probe theory)

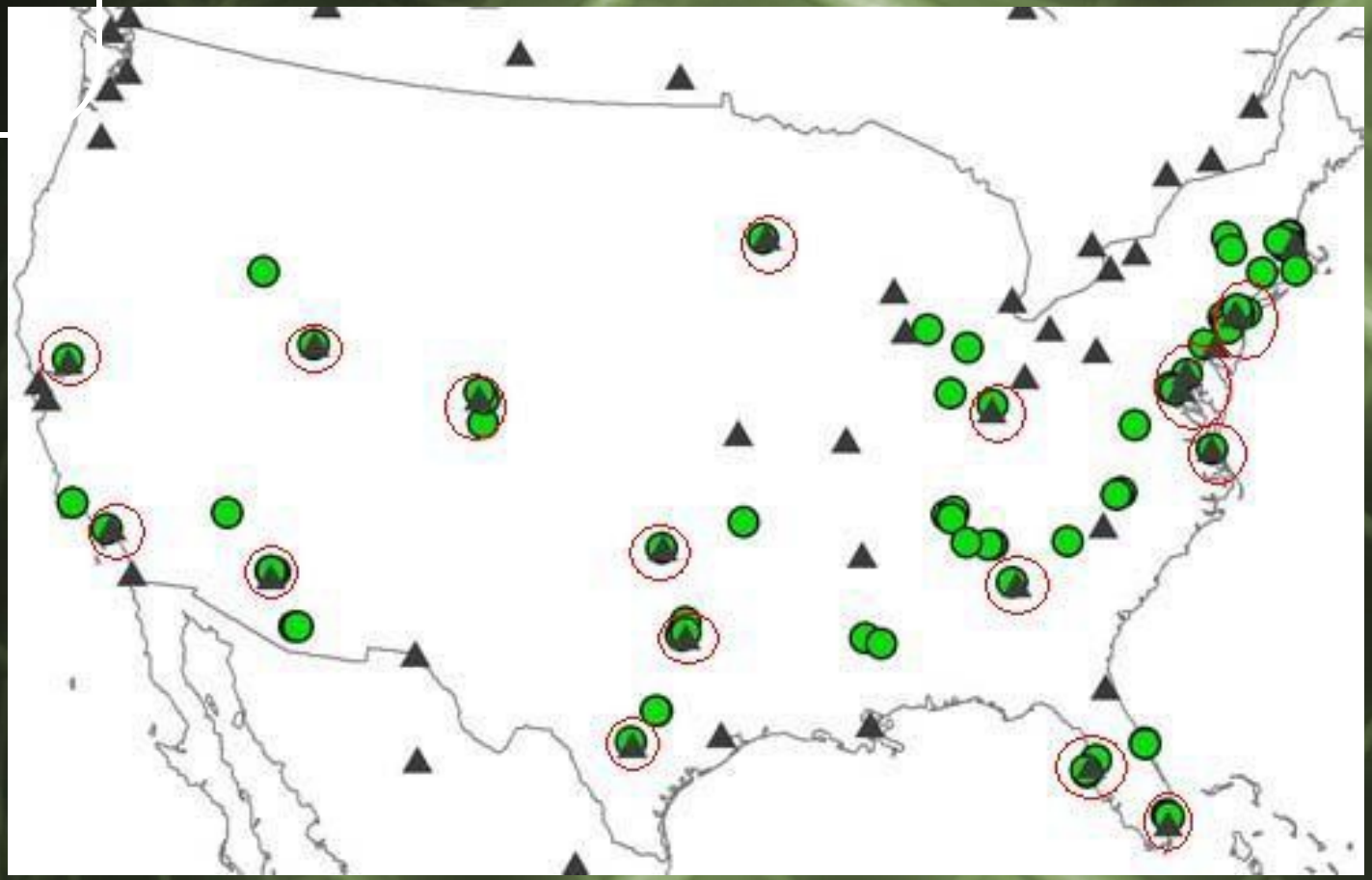


2. Eliminate ‘friendlies’

Map Legend

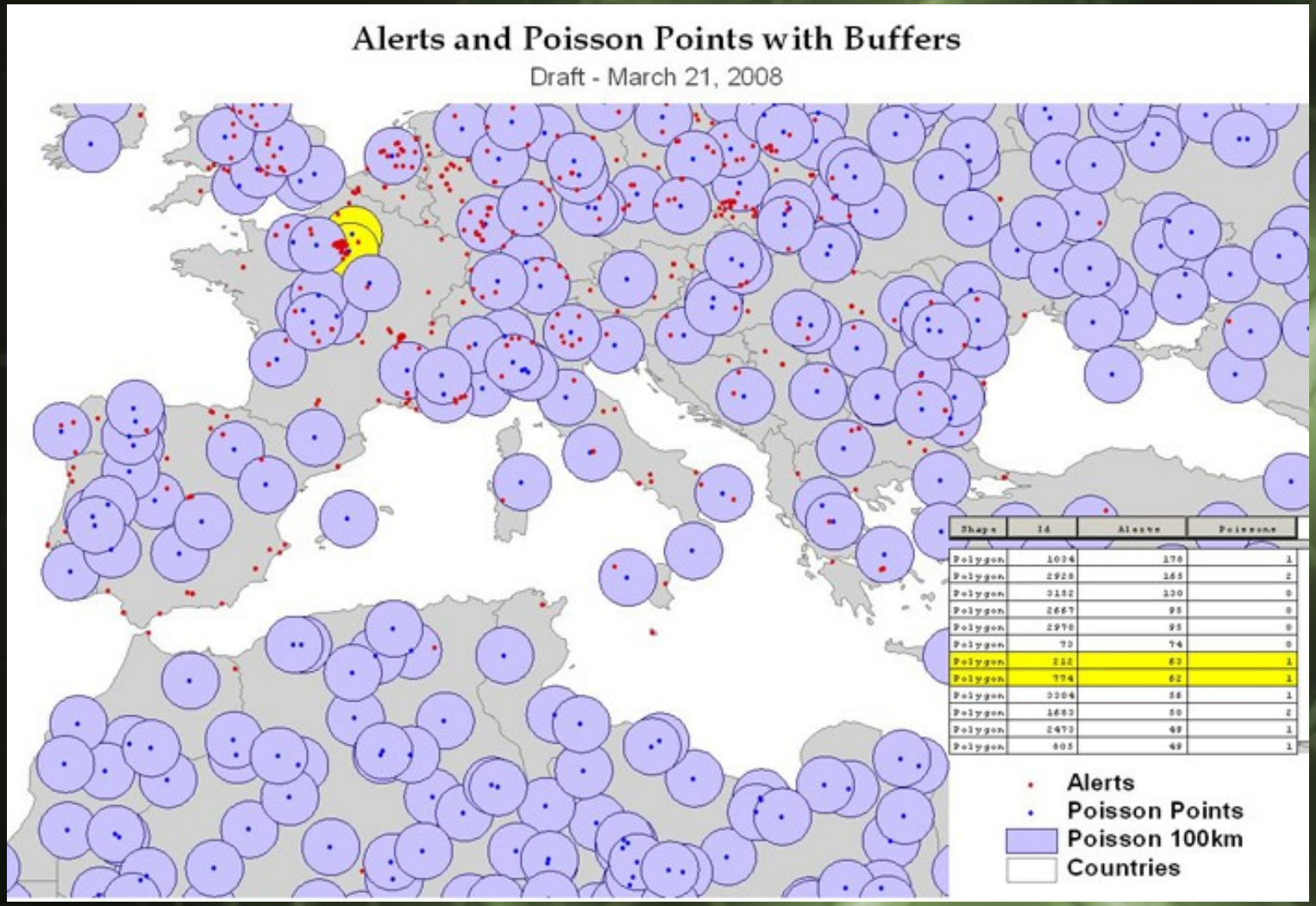
= Source IDS Alert

= Remote Offices or Telecommuting Residences

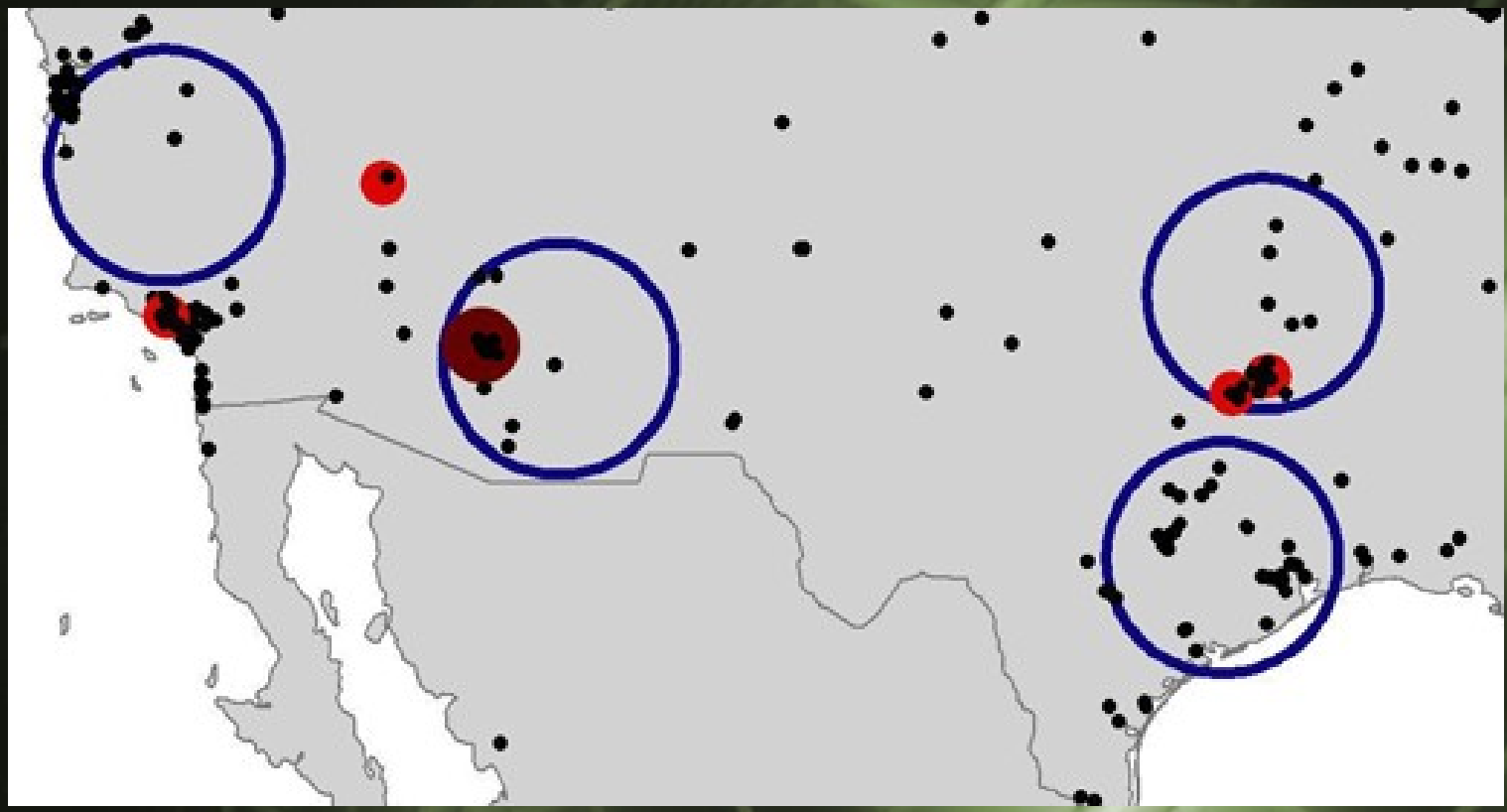


Depending on your risk comfort abilities this would eliminate ~30% of potential false positives.

3. Run a GIS clustering algorithm



4. Extract ‘hot-spot’ network alerts



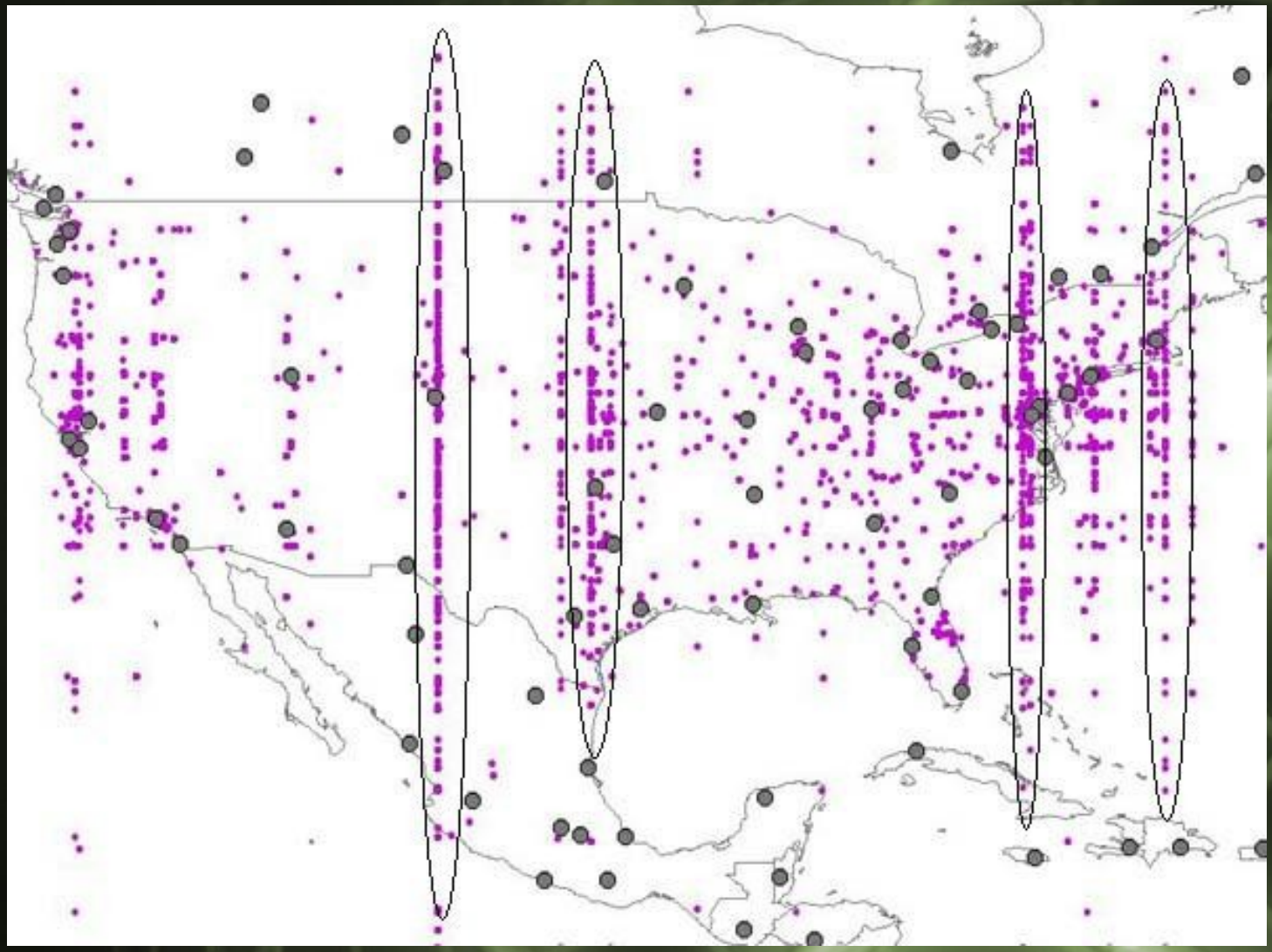
5. Run a weight calculating algorithm to evaluate if there is a relationship between alerts

- Insert image(s) later…

Accuracy translation

- Vendors
  - IP2Location
  - MaxMind
  - Quova (wireless capabilities)
- How is the translation calcuated?
  - Domain scrapping
  - Compare Traceroutes
  - Strategic partnerships with ISPs
  - Strategic partnerships with downloading FTP sites

Example of ‘less’ accurate translation



Okay…how do I beat it?

- As with many (if not all) defenses there are always loopholes:
  - Most scanning/enumeration tools primarily do sequential scans of IP address – DO NOT USE SEQUENTIAL IPs TO ATTACK A VICTIM
  - Map remote locations and use a tool to extract neighboring IP addresses – which will hopefully get extracted when eliminating ‘friendlies’
  - Attack from random geographic locations and with varying times

Deconstruct the translation file

- Insert image of deconstructed application

Q&A

Back to the Guinness tap…