



Bad guys are everywhere,
good guys are somewhere!

NSA/CSS Threat Operations Center (NTOC)
NTOC Technology Development



(U) NTOC



- (U//FOUO) Operates under *both* SIGINT and Information Assurance authorities
 - Leverage SIGINT, IA, OSINT
- (U//FOUO) Coordinates Integrated Cyber Operations
 - V2: Analysis
 - V3: Operations
 - V4: Technology Development Support
 - V45: Technology Development Division



(U) V45 - Projects



TREASURE MAP

- (U//FOUO) TREASUREMAP
 - Massive Internet mapping, exploration, and analysis engine
- (U//FOUO) PACKAGEDGOODS
 - Globally dispersed traceroute generators
- (U) Other Projects





(U) What is TREASUREMAP?

(U//FOUO) Capability for building a near real-time, interactive map of the global internet.

Map the entire Internet – Any device*, anywhere, all the time

(U//FOUO) We enable a wide range of missions:

- Cyber Situational Awareness – *your own network plus adversaries'*
- Common Operation Pictures (COP)
- Computer Attack/Exploit Planning / Preparation of the Environment
- Network Reconnaissance
- Measures of Effectiveness (MOE)

(* limited only by available data)

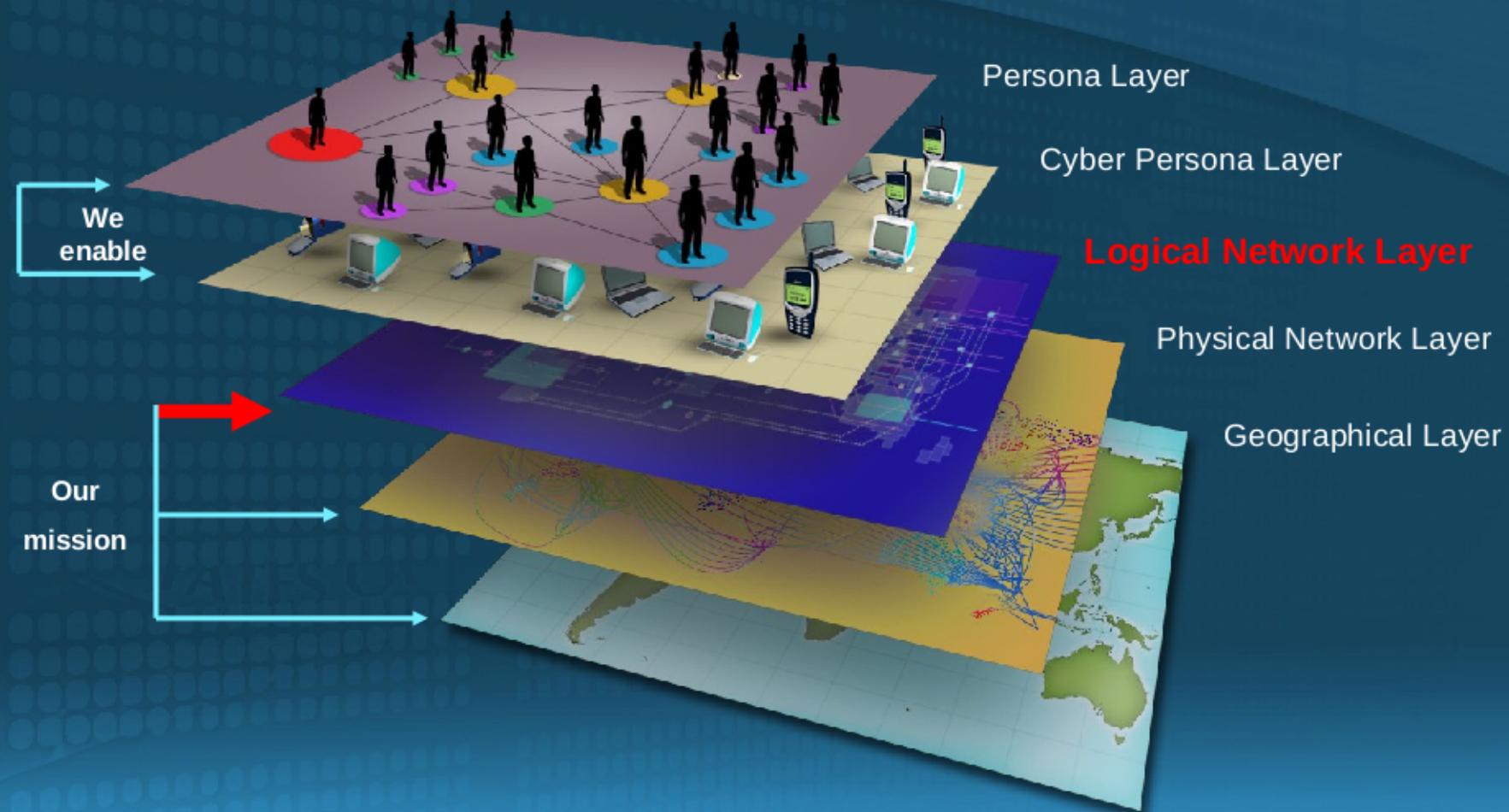


(U) TREASUREMAP

- (U//FOUO) Continual generation of global Internet map, IPv4 and IPv6 (limited)
- (U//FOUO) Focus on logical layers (router and autonomous system), but touches physical, data link, and application layers
- (U) Its Huge.



(U) TREASUREMAP as an Enabler





(U) Current State

- (U//FOUO) Data Sources
 - Open Source Intelligence (OSINT) * & Academic
 - Commercially Acquired
 - SIGINT
 - Information Assurance
- (U//FOUO) Available on multiple networks to many user groups
 - NSAnet – TREASUREMAP (TM)
 - 5-Eyes partners
 - JWICS users - USG IC
 - SIPRNet – USG IC /DoD – TREASUREMAP-SIPR (TM-S)
- (U) New capabilities delivered every 90 days
- (U) 30+ Gigabytes of additional data added and replaced per day

(* OSINT – Open Source / Publicly available Internet Meta-Data)



(U) Data Sources

Feed the Machine



(U) OSINT, Commercial & Academic

- (U//FOUO) BGP
 - Gives the 300,000 foot view of the Internet
 - Defines routing across Autonomous Systems (AS)
 - Origination of IP address spaces (Prefixes) to AS
 - How the Internet gets knowledge of itself (IP address space)
 - Commercially purchased Data Sources
 - Akamai, SOCIALSTAMP, SEASIDEFERRY
 - Open Source
 - Public BGP, IXP (RIPE), APNIC, ROUTEVIEWS, CERNET



(U) OSINT, Commercial & Academic

- (U//FOUO) Traceroutes
 - Router –to- router links to targeted IP addresses
 - Creates links between networking devices (routers)
 - TM ingests approx. ~16–18 million traceroutes daily
 - Gives the 300 foot view, router-to-router infrastructure
 - Data Sources
 - ARK – CAIDA's Archipelago Project *
 - PACKAGEDGOODS *
 - SOCIALSTAMP
 - RUSTICBAGGAGE
 - User Input



(U) OSINT, Commercial & Academic

- (U) Registries - Information on netblock and AS ownership
- (U) DNS - IP address to domain name matching
- (U) Operating System (OS) Fingerprints
 - Software and Operating System characteristics of networked devices
 - ~30-50 million unique IP addresses represented per day



(U//FOUO) Traceroutes: PACKAGEGOODS

- (U//FOUO) Collects “network measurement” data, on public internet
- (U) Random traceroutes and user requested
- (U//FOUO) **PG-GTR**
 - Currently using ~700 public traceroute sites to perform operations
 - High target (full IP addresses)
 - Capable of ~4K IPv4 and IPv6 traceroutes daily
- (U//FOUO) **PG-Server**
 - High volume: ~6.5 million traceroutes per day
 - Low targeting: IPv4 /24 netblocks or higher
 - Can do whole ASes, Country, Netblocks
 - 13 covered servers in unwitting data centers around the globe
 - **Asia:** Malaysia, Singapore, Taiwan, China (2), Indonesia, Thailand, India
 - **Europe & Russia:** Poland, Russia, Germany, Ukraine, Latvia, Denmark
 - **Africa:** South Africa
 - **South America:** Argentina, Brazil



(U) Coming Soon!

- (U//FOUO) **PG-Server 2.0**
 - Tasking of full IP address
 - Choice of traceroute types:
 - ICMP
 - ICMP Paris
 - TCP
 - UDP
 - Choice of PG-SVR (for source of traceroute)
 - Auto-refresh



(U) Traceroutes - CAIDA

- (U) University of California, San Diego
 - Cooperative Association for Internet Data Analysis
 - Archipelago measurement platform
- (U//FOUO) TM data source: ARK
- (U) High volume: ~10 million traceroutes per day
- (U) Random targeting (/24 netblock, BGP advertised)
- (U) 44 Locations: Asia (5), Europe (15), Africa (2), North America (18), South America (2), Oceania (2)



(U) Internal Sources (Protected Sources)

- (U//FOUO) **PACKAGEDGOODS - NTOC**
 - (S) Clandestine traceroute and DNS processor
- (S//SI//REL) **BLACKPEARL – NAC**
 - SIGINT session 5-tupel, identified routers, routing protocols, SIGINT access points, (inferred SIGINT access points)
- (S//SI//REL) **LEAKYFAUCET – NAC**
 - Flow repository of 802.11 WiFi IP addresses and clients via STUN data
- (S//SI//REL) **HYDROCASTLE – NAC/INSCOM**
 - 802.11 configuration data extracted from CNE activity in specific locations
 - (Requires HYDROCASTLE account)
- (S//SI//REL) **MASTERSHAKE – NAC**
 - FORNSAT and WiFi collection data
- (S//SI//REL) **S-TRICKLER - NTOC**
 - IP address fingerprints and potential vulnerabilities from FORNSAT collection



(U) Internal Sources (Protected Sources)

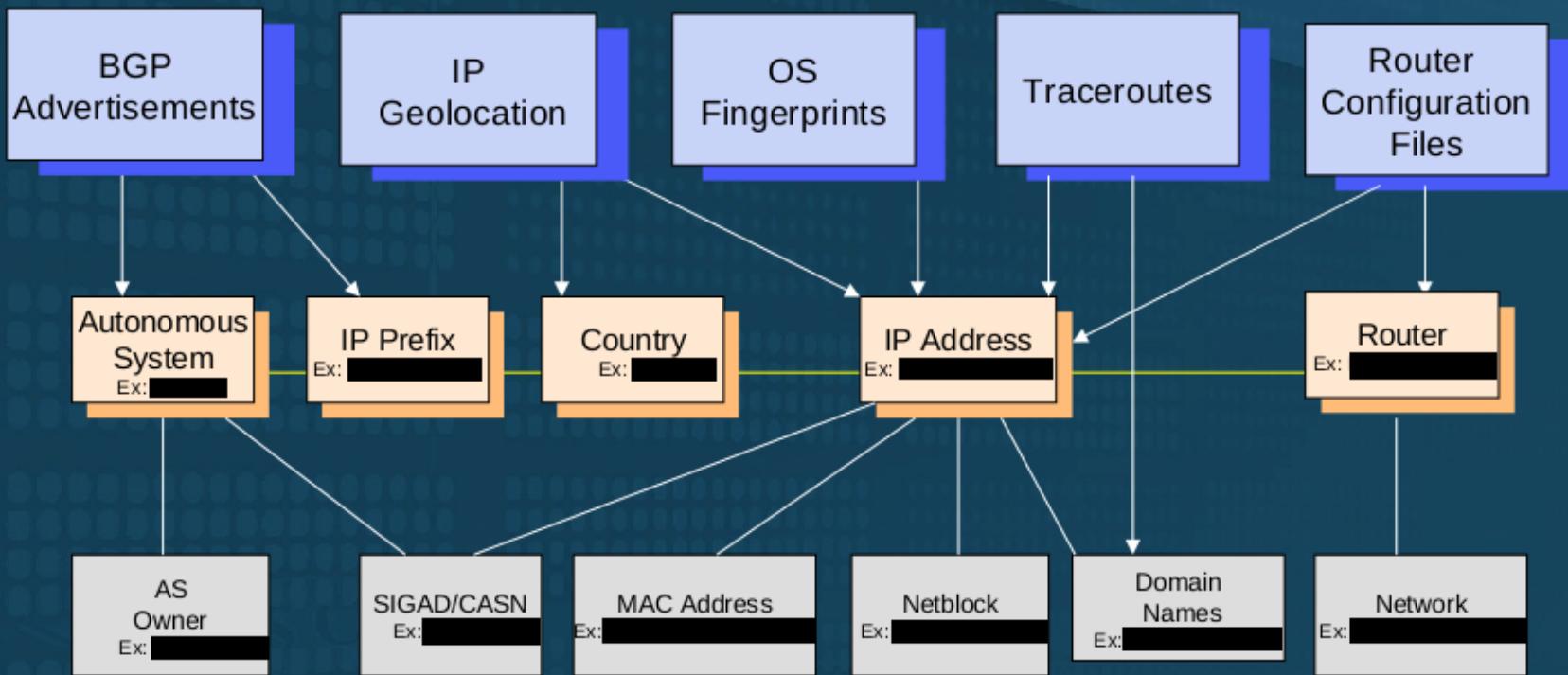
- (S//SI//REL) **TOYGRIPPE** - NAC
 - Repository of VPN endpoints
- (S//SI//REL) **DISCOROUTE** – NAC/GCHQ
 - Router configuration files from CNE and passive SIGINT
 - NAC's DISCOROUTE repository
- (TS//SI//REL) **VITALAIR2** – TAO
 - Automated scanned IP addresses for TAO known vulnerabilities
- (U//FOUO) **IPGeoTrap** - NAC
 - Provides geolocation services for IP addresses/ranges
- (TS//SI//REL) **JOLLYROGER** – SSG/TAO
 - Provides metadata that describes the networking environment of TAO-implanted Windows PCs
 - (Requires JOLLYROGER account)
- (U//FOUO) **TUTELAGE** – NTOC
 - Specific alerts from intrusion detection sensors
 - (not currently active)



(U) The Whole is Greater than the Sum of the Parts



(U) Data Relationships

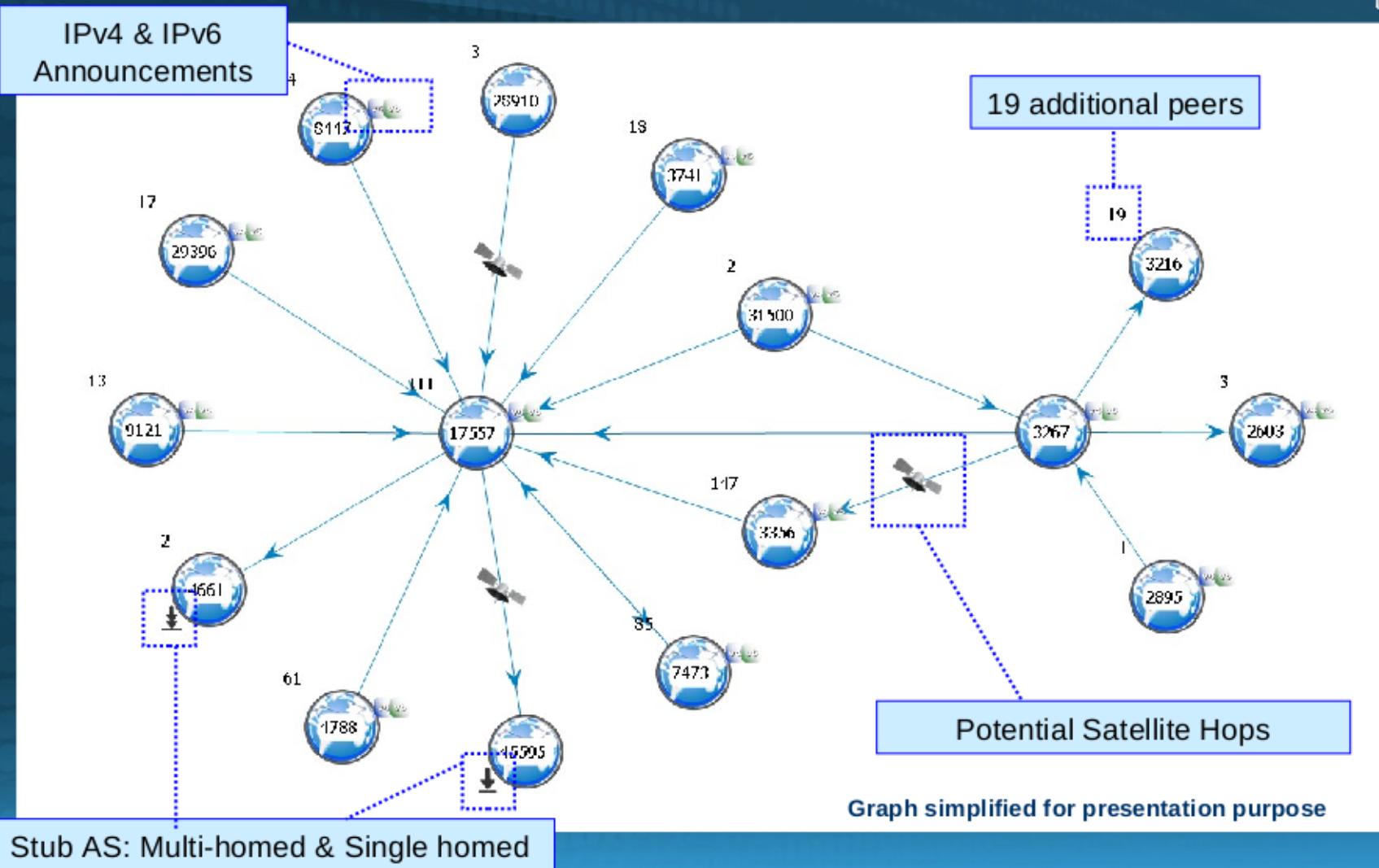


Yellow links denotes direct relationships between data types.

For example, we know which AS contains a router because we can relate a router to IP Addresses, IP Addresses to IP Prefixes, then IP Prefixes to an AS.



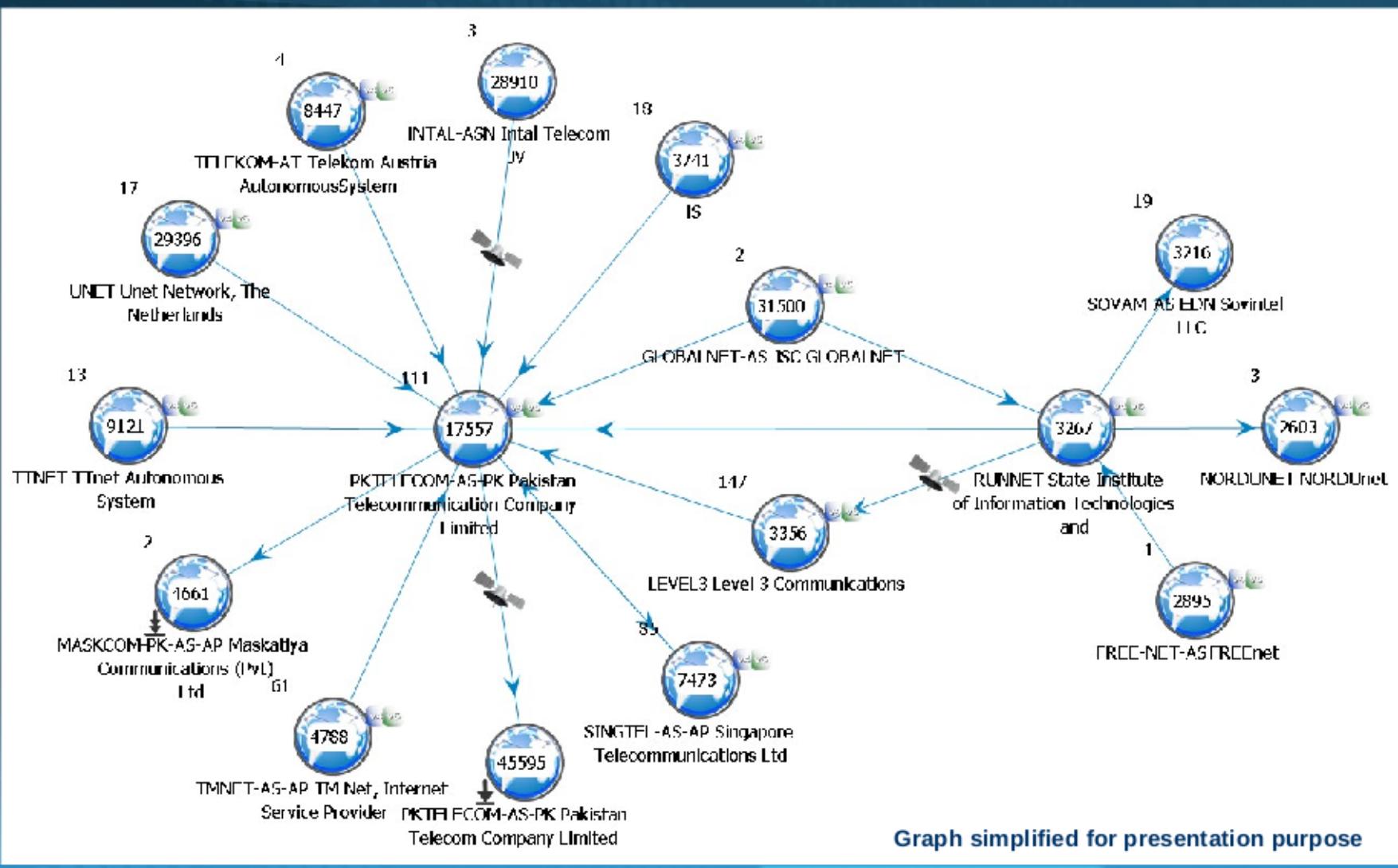
(U) Autonomous System Peering - BGP



Stub AS: Multi-homed & Single homed

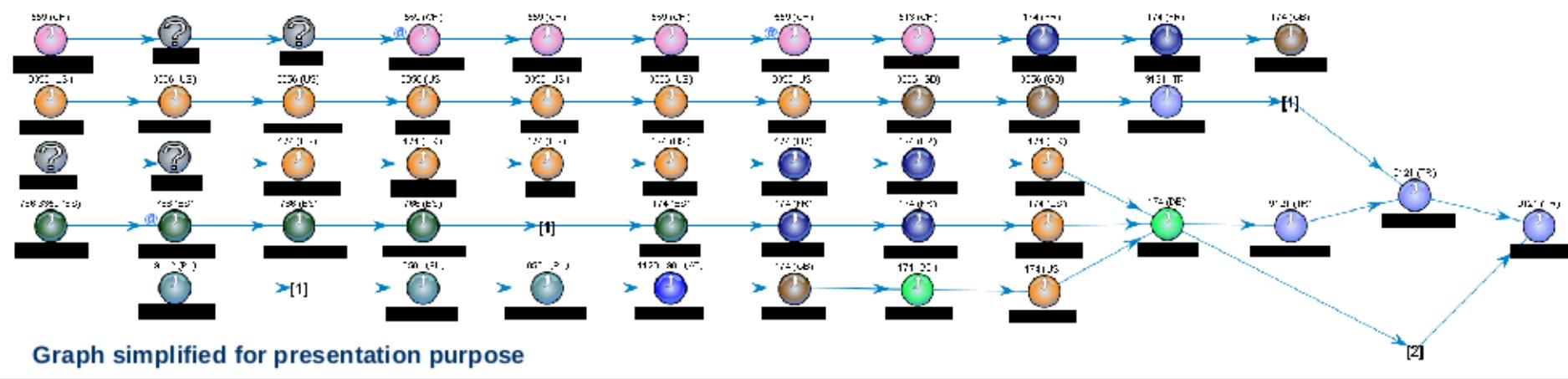


(U) ... and Registries





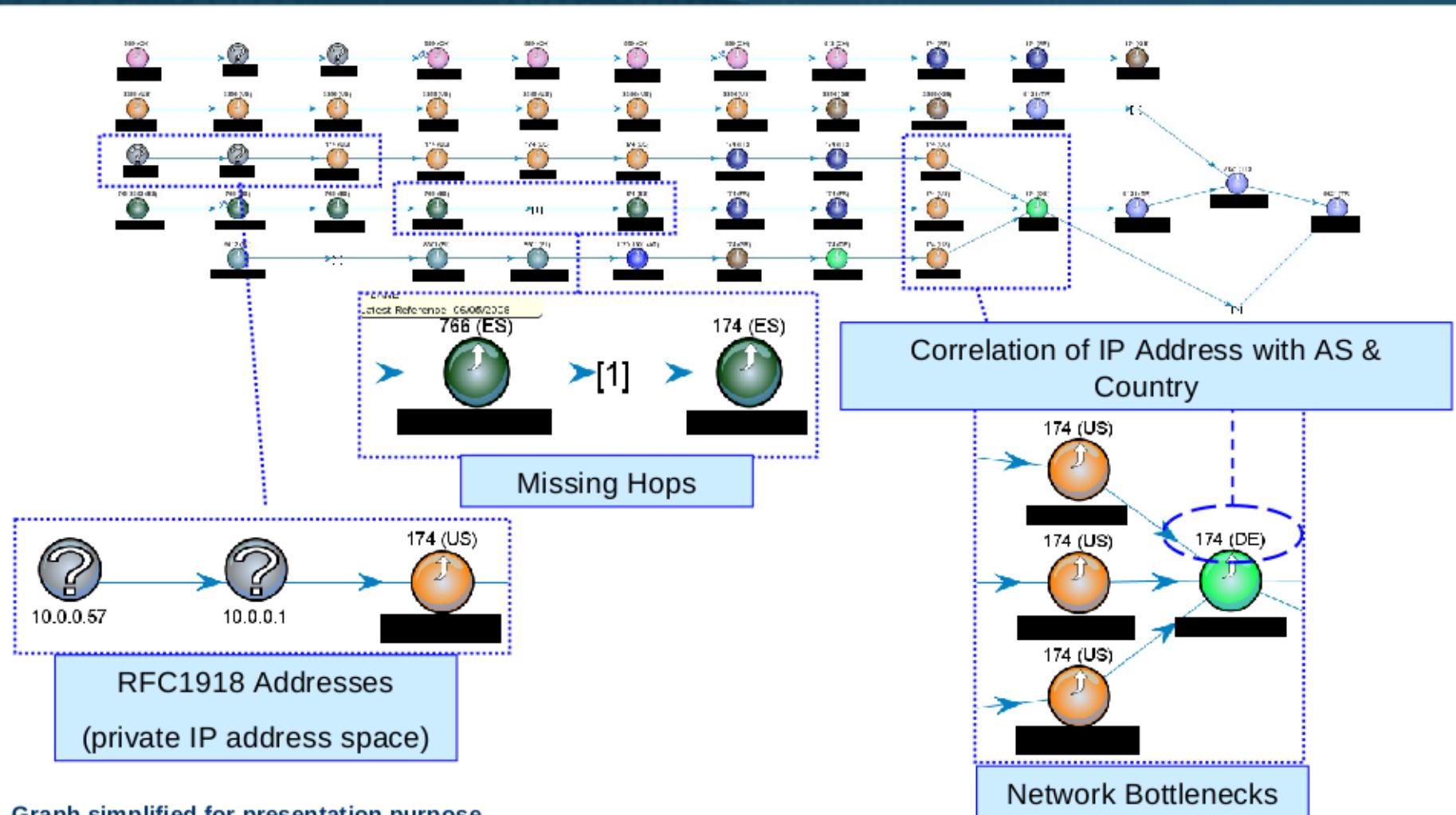
(U) Internet “flow” to a “Network”^{1B}



They're color-coded by country. Big deal.



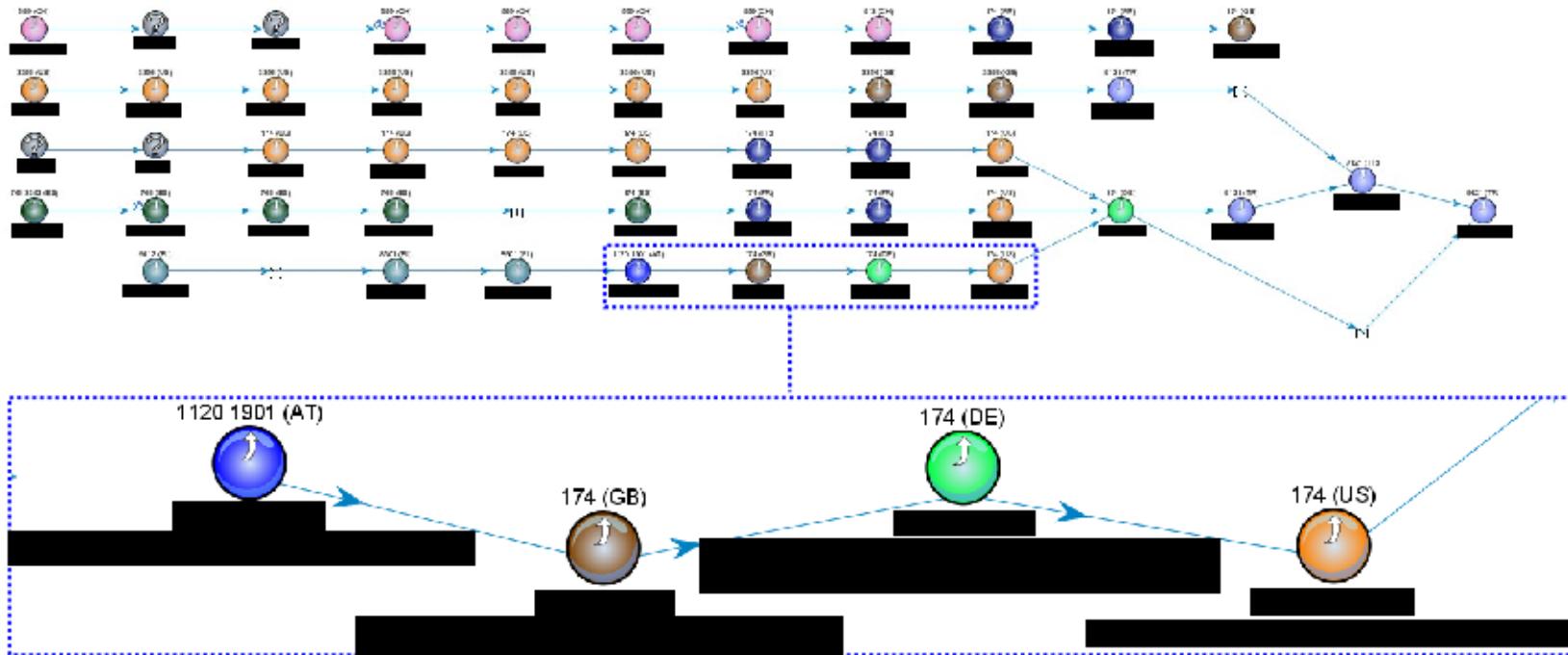
(U) With Traceroute...



Graph simplified for presentation purpose



(U) ... and DNS



Graph simplified for presentation purpose



(U) IP Geolocation Data



- Correlate IP addresses with country, latitude and longitude (via IPGeoTrap)





TS//SI//REL TO USA, FVEY



(U) Seeing Red

SIGINT in the Water

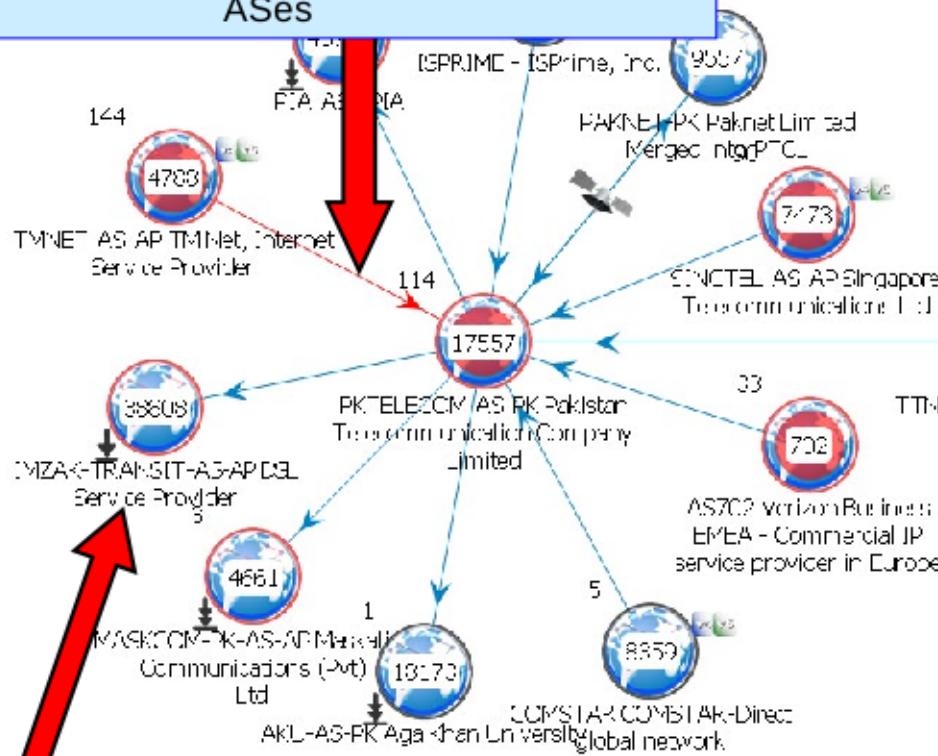
TS//SI//REL TO USA, FVEY



(S//SI//REL) Bring the SIGINT (AS Level)

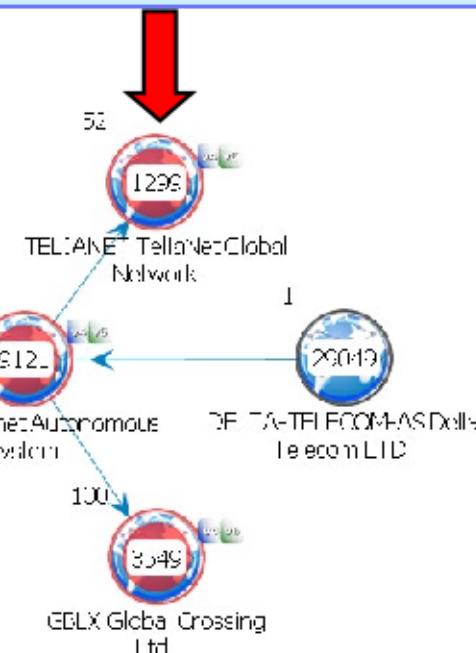
Red Links:

SIGINT Collection access points between two ASes



Red Core Nodes:

SIGINT Collection access points within AS



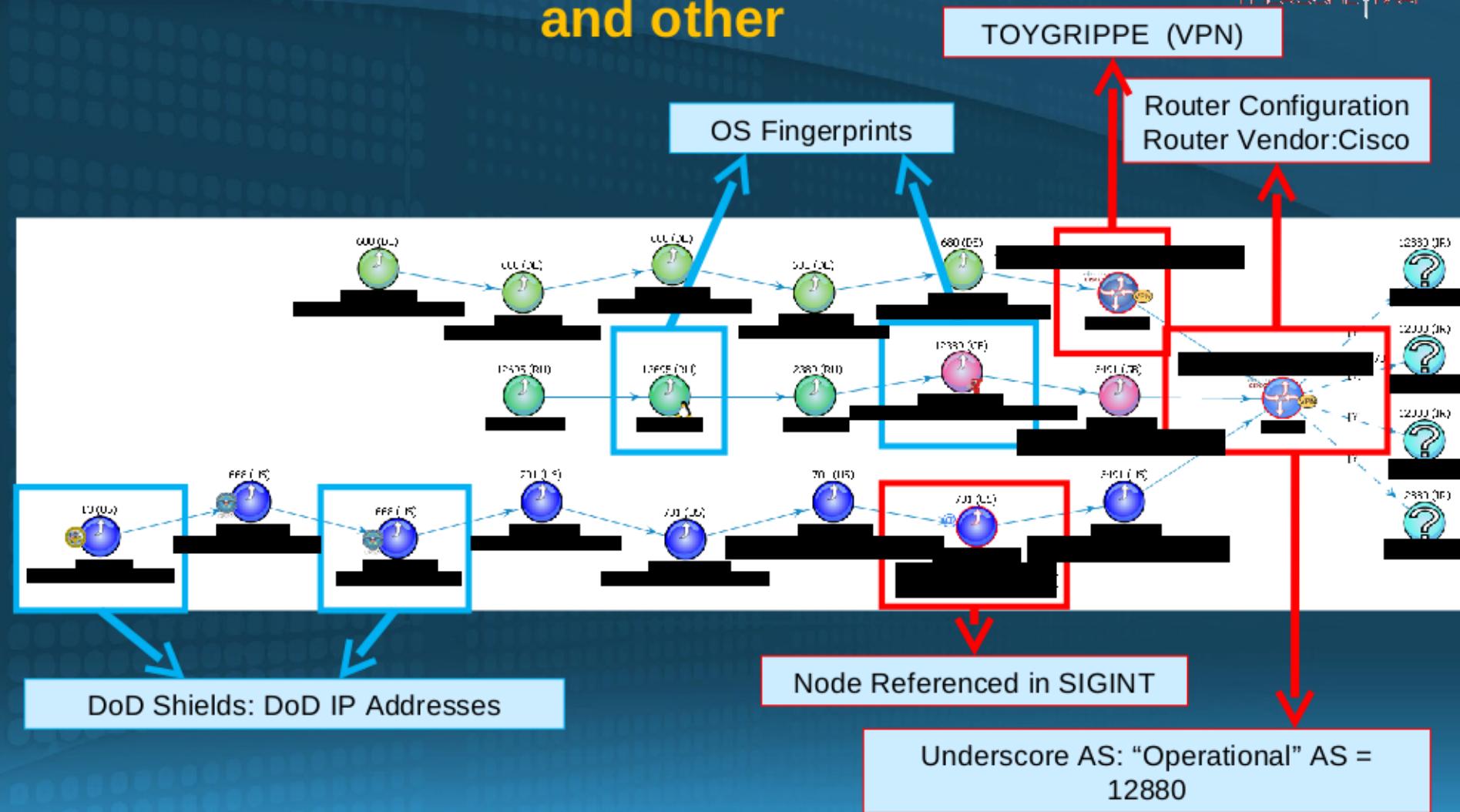
Red Ringed Node:

Nodes within AS are SIGINT Referenced

Graph simplified for presentation purpose



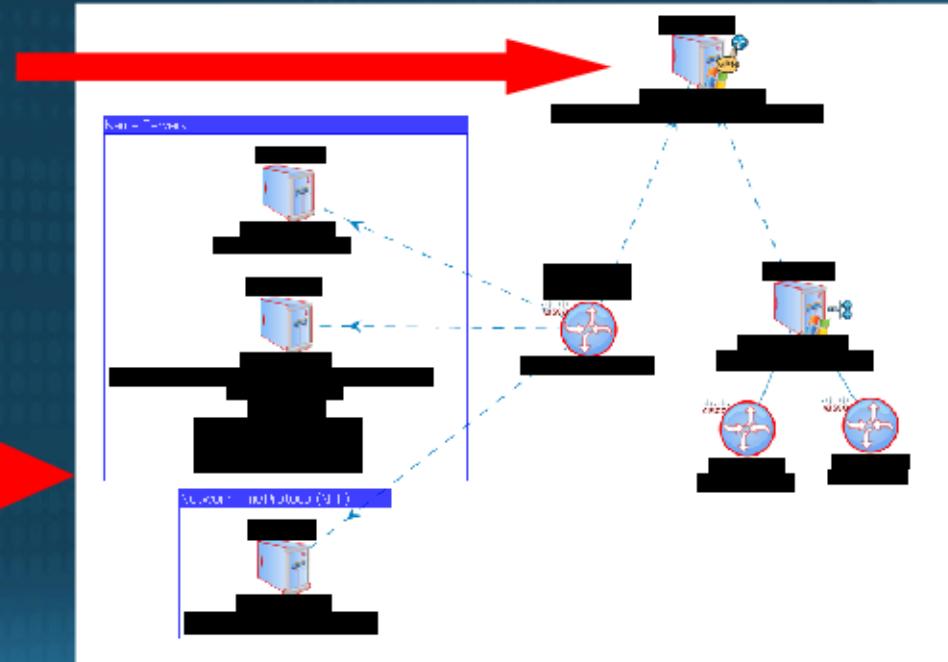
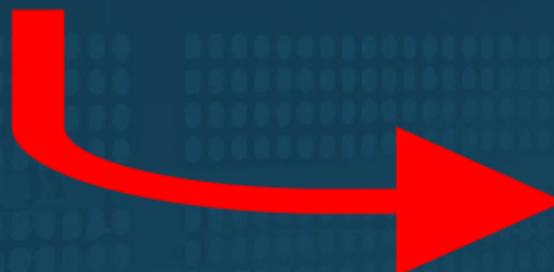
**(S//SI//REL) Traceroute – overlaid with SIGINT
and other**





(S//SI//REL) Known Devices

- (S//SI//REL) Sources: DISCOROUTE (NAC router configuration repository)
- (S//SI//REL) Display supporting infrastructure, as configured in router configuration files
 - Where router accessed from (possible NOC?)
 - servers configured for router (NTP, DNS, Radius, TACACS)





(S//SI//REL) Known Devices



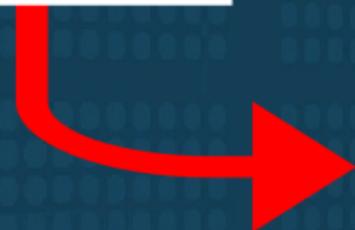
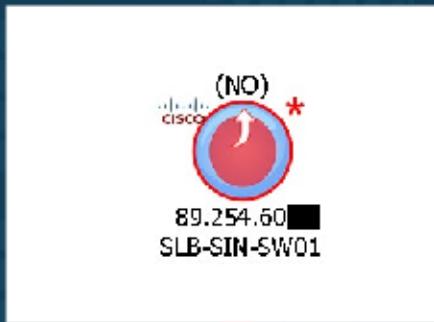
- (S//SI//REL) Sources: DISCOROUTE (NAC router configuration repository)
 - (S//SI//REL) Router data in tables

Show Brothers Accessed from [REDACTED]		[REDACTED] 09/09/2010 12:00:00 AM			
Accessed From	Accessed To	Access Date	Protocol	Locd	Last
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

```
spawm_wldj
media_type:mpeg
no_cop_protection
avg_bitrate:100
1
```



(S//SI//REL) Cisco Discovery Protocol (CDP)



CDP Router Report: SLB-SIN-SW01

```
---  
Date: 05/04/2011  
Device Name: SLB-SIN-SW01  
Model: cisco WS-L2960-24TC-L  
Capabilities: Performs Level2 Switching  
     ISMRP Flag Set  
Software Version: 12.2(25)SEZ  
Network Prefixes: -  
Duplicate Ports: -
```

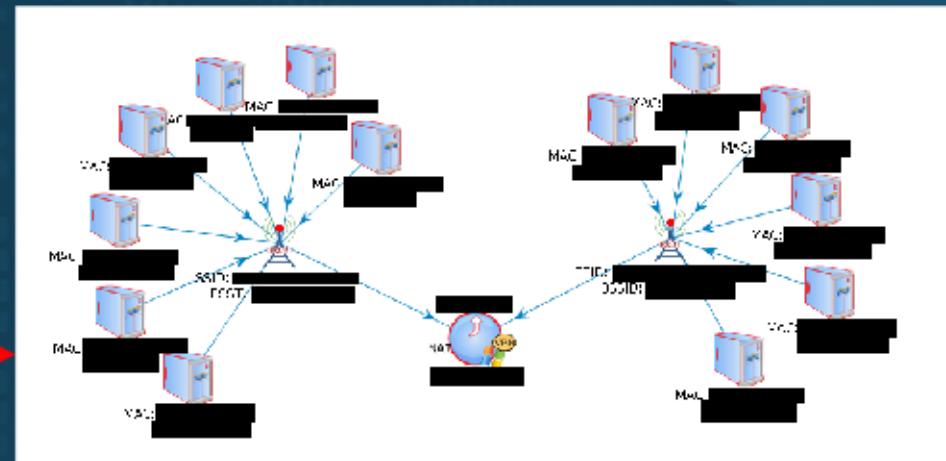
Physical Port	Address	Protocol	AS	Country	Data Sources
FastEthernet0/6	89.254.60.0	IP	N/A	NORWAY	ED_REL [05/03/2010 20:00:00]



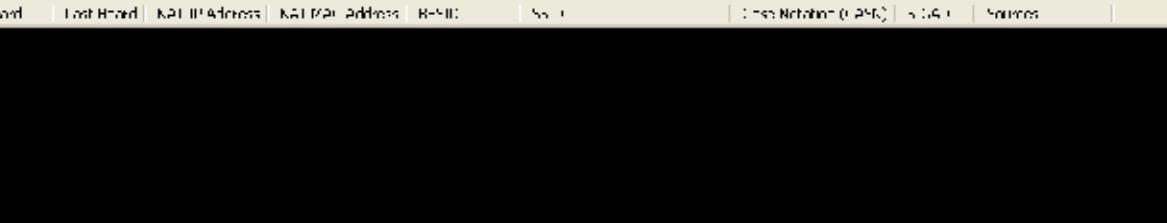
(U//FOUO) 802.11 WiFi Data



- (U//FOUO) Display and correlation of 802.11 wireless networks and RFC1918 clients
 - (S//SI//REL) Sources
 - HYDROCASTLE *



TOP SECRET//COMINT//REL TO LSA, FvEX//203201

Wireless Report [REDACTED] (originally generated on 5/9/2010 at 12:22 EDT)	
First Board Last Board KAT IP Address KAT MAC Address R-SID <input type="button" value="Save"/> <input type="button" value="Clear Selection (0 PSC)"/> <input type="button" value="Print"/> <input type="button" value="Sources"/>	
	

(* HYDROCASTLE account required)



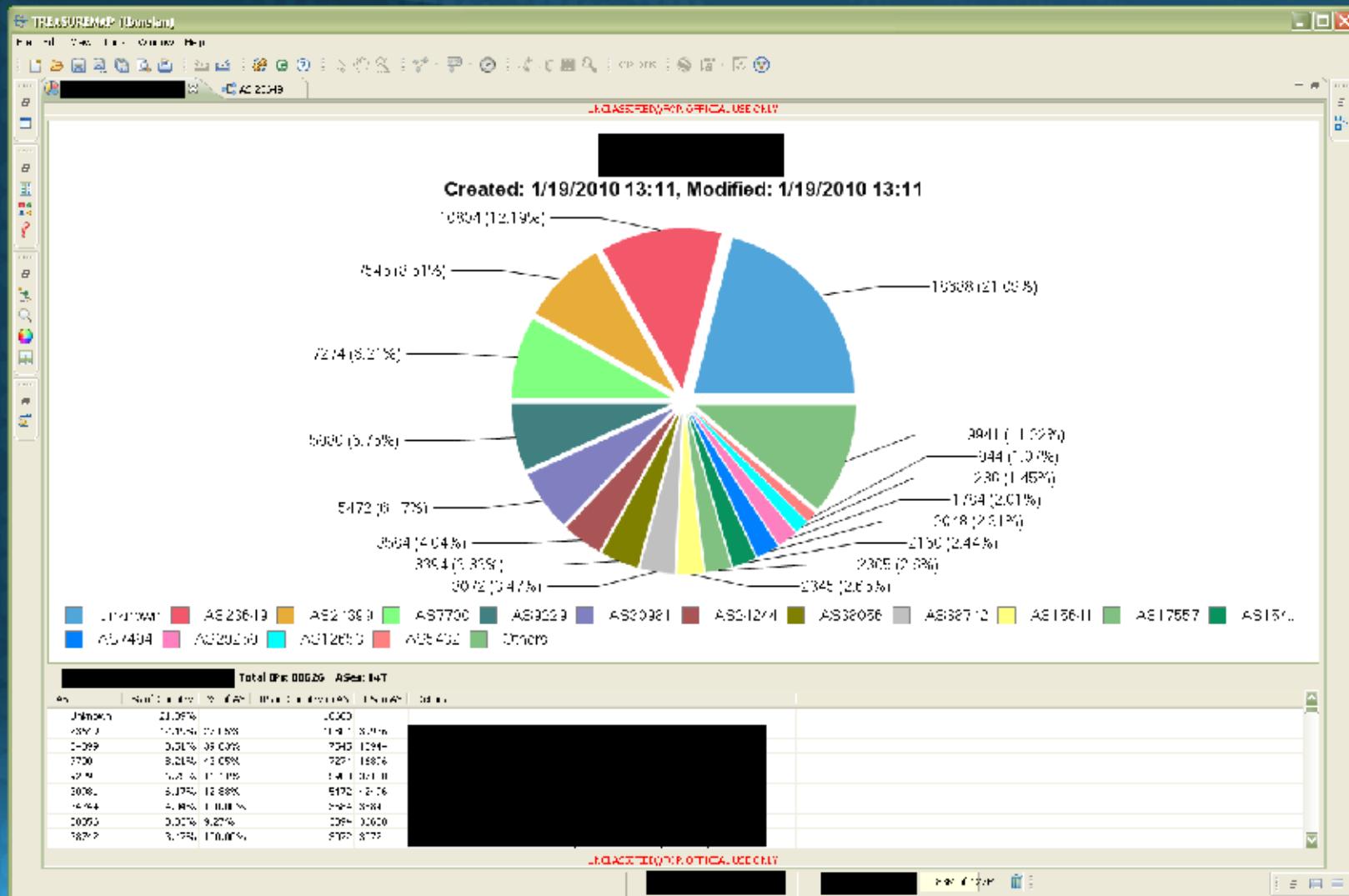
(U) Communities

- (S//SI//REL) Individual IP addresses related by a common attribute
 - TOR router
 - Servers (DNS, NTP, SNMP, TACACS, RADIUS)
 - Hide IP NG Proxy Servers
 - BYZANTINE HADES Infrastructure hosts/infected hosts
- (S//SI//REL) Sources: (Varies)
 - Currently TOR router advertisements
 - router configurations
 - XKEYSCORE





(U) Country (AS Presence)





(U//FOUO) TREASUREMAP Workspace

- (U//FOUO) **Toolbar**: Offers access to a variety of commonly used functions
- (U//FOUO) **Search Pane**: Input search parameters
- (U//FOUO) **Advanced Search Options**: Preferences for searches
- (U//FOUO) **Release my search to PG**: Requesting traceroutes for target IP addresses
- (U//FOUO) **Other Searches**: Includes Router, DNS, Batch IP/MAC and JOLLYROGER
- (U//FOUO) **Legend**: Contains all of the icons and decorations as seen in an active graph
- (U//FOUO) **Send Feedback**: Provides a way to communicate questions, comments or problems to the TREASUREMAP team.

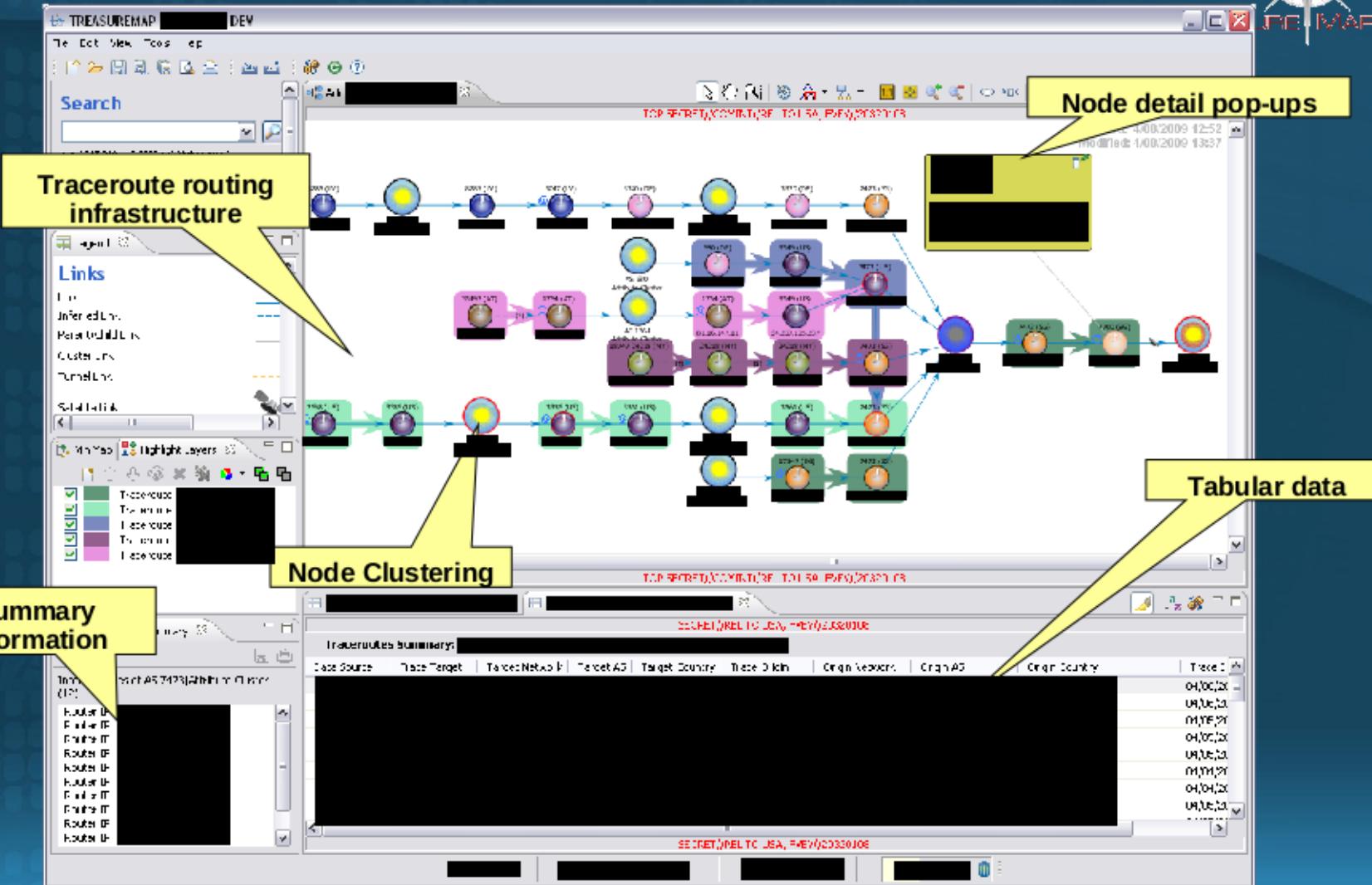


(U//FOUO) TREASUREMAP Search Items

1. (U//FOUO) IP Address
2. (U//FOUO) Routers
3. (U//FOUO) DNS (FQN)
4. (U//FOUO) MAC address / 802.11 BSSID / 802.11 SSID
5. (U//FOUO) IP Prefix / Range (CIDR Notation)
6. (U//FOUO) Registry Netblock
7. (U//FOUO) SIGAD and/or Case Notation
8. (U//FOUO) Country / IP Country Code
9. (U//FOUO) Autonomous System (AS) Number
10. (U//FOUO) Free Text



(S//SI//REL) User Interface: NAVS





(UFOUO) User Interface: Website



Cyrus Key - Black Hawk (Qualified User TS//SI//REL TO USA, FVEY)

TREASUREMAP
[Build ESU](#) | [Quick Start](#) | [FAQ](#) | [Release Notes](#)

[Home](#)
[Query](#)
[Users](#)
[Packaged Goods](#)
[Data](#)
[Tools](#)
[Gallery](#)

[Run on TREASUREMAP](#)
[Go](#)

(INFO/FOUO) On Friday, 28 February 2008 at approximately 1600 EST, TREASUREMAP Application option is disabled. If running a shared installation please contact your system administrator. To continue with the new version, select "Proceed with Update" when prompted. If you chose a shared installation, software reversion occurs. To continue using the current version select "Work Online without Upd." until your system administrator can update you to the current version.

Small text-based queries

Enter Number, IP Address, IP Prefix, or Country:

Video Tutorials

Click here to learn how to use this feature

- ▶ [How To Find A File](#)
- ▶ [How To Delete A File](#)
- ▶ [How To Import Data](#)
- ▶ [How To Delete An IP Prefix](#)
- ▶ [How To Find An IP Prefix](#)
- ▶ [How To Perform A Search Using Advanced Search](#)
- ▶ [How To Perform A Search Using Basic Search](#)
- ▶ [How To Delete A Search Result](#)
- ▶ [How To Create A Search Result](#)
- ▶ [How To Export Google Search](#)

On-line Help

URLS/URID/URID Help Block



Customer Level: [REDACTED]
Customer Service Team: [REDACTED]

TREASUREMAP F12 New Features

- ▶ New data sources to analyze, network analysis and data, transaction and activity data.
- ▶ New capability to view 10 New Fingerprint Data Records from the new Fingerprint Details tab.
- ▶ New functionality to Extract Recently Used Queries.
- ▶ New capability to View and Export F12 of M4444 Transaction ID from Activity.
- ▶ New file import since within the Google open file feature.
- ▶ New ability to Identify Next Trendy on a graph to quickly identify critical trend points.
- ▶ Improved Sorting capabilities.
- ▶ New PMS Network Search capabilities.
- ▶ New and improved Look and Feel of the TREASUREMAP Web site.
- ▶ New Search Functionality to search in the TREASUREMAP Website and help contents and quickly find what you need.
- ▶ Enhanced Charting capabilities.
- ▶ TREASUREMAP CDRs Calculator now supports IF126 portlets.
- ▶ New choice of themes to assist in changing your color mode.



(U//FOUO) TREASUREMAP Contact Info

- [REDACTED]
 - Government Lead
 - [REDACTED]
- Customer Support Team
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
- Email: DL
 - [REDACTED]
 - [REDACTED]