

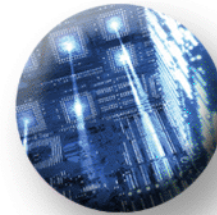
ManTech

International Corporation

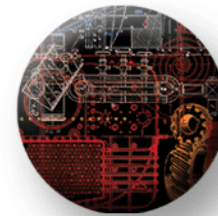
Leading the Convergence of
National Security and Technology



Secure Systems
and Infrastructure
Solutions



Information
Technology
Solutions



Systems
Engineering
Solutions



Internet Based Reconnaissance Operations

Overview

- Who we are
- What we provide
- Examples of work
- NetTroll
- Summary



ManTech SMA



“Making America Stronger by Supporting and Securing Critical Missions”

- ✓ **Intelligence Operations Support**
- ✓ **Secrecy Architecture/Lifecycle Security Support**
- ✓ **Computer Forensics & Intrusion Analysis**
- ✓ **Counterintelligence Support Services**
- ✓ **Network Engineering Services**
- ✓ **SIGINT Systems Life Cycle Engineering**
- ✓ **Advanced Decision Support Systems Development**

What is Internet Based Reconnaissance?

- Traditionally Internet-based OSINT efforts
 - Keyword-only searches miss similar subject matter
 - Standard web searches often don't find short-lived information
 - Do not correlate other aspects of available data
- ManTech CFIA Internet-Based Reconnaissance
 - OPSEC and Mission First!
 - Use of open source collection techniques paired with customized toolsets
 - Non-attributable architecture; small footprint
 - Can be as widely or narrowly focused as needed
 - Combination of Intel analysts with experienced network engineers
 - Extensive network backgrounds
 - Native language searching
 - Rapid turnaround time
 - Iterative process working with the customer to constantly drive research

What do we provide our Customers?

- Locate / Profile Internet “Points of Presence”
 - Individuals
 - Companies
 - ISP’s
 - Organizations
 - Items of Interest
- Detailed network mapping
 - Identify registered networks and registered domains
 - Graphical network representation based on Active Hosts
 - Operating system and network application identification
 - Identification of possible perimeter defenses
- Technology Research
- Intelligence Gap Fill
- Counterintelligence Research
- Customer Public Image Assessment



What is our Process?

- Employ highly skilled network professionals
- Use Non-attributable Internet access
- Use custom developed toolsets and techniques
- Use Native Language and in-country techniques
 - Utilize foreign language search engines, mapping tools, etc
- Utilize iterative researching methodologies
- What we search:
 - Websites, picture sites, mapping sites/programs
 - Blogs and social networking sites
 - Forums and Bulletin Boards
 - Network Information: Whois, Trace Route, NetTroll, DNS
 - Archived and cached websites



What do we Produce?

- Rapid Non-attributable Open Source Research Results
 - Sourced Research Findings
 - Triage level Analysis
 - Vulnerability Assessment
 - Graphical Network and Social Diagramming

How does Internet Based Reconnaissance Fit into the “Big Picture”?

- Allows you to better understand your program’s public profile
- Provides decision-making information
- Determines the status of foreign programs
- Fills the gaps in understanding
- Removes traditional “High-side blinders”



Example: Actor Dossier

TASK - Research the actor “sn33kydvl”

Found a personal website with multiple photos



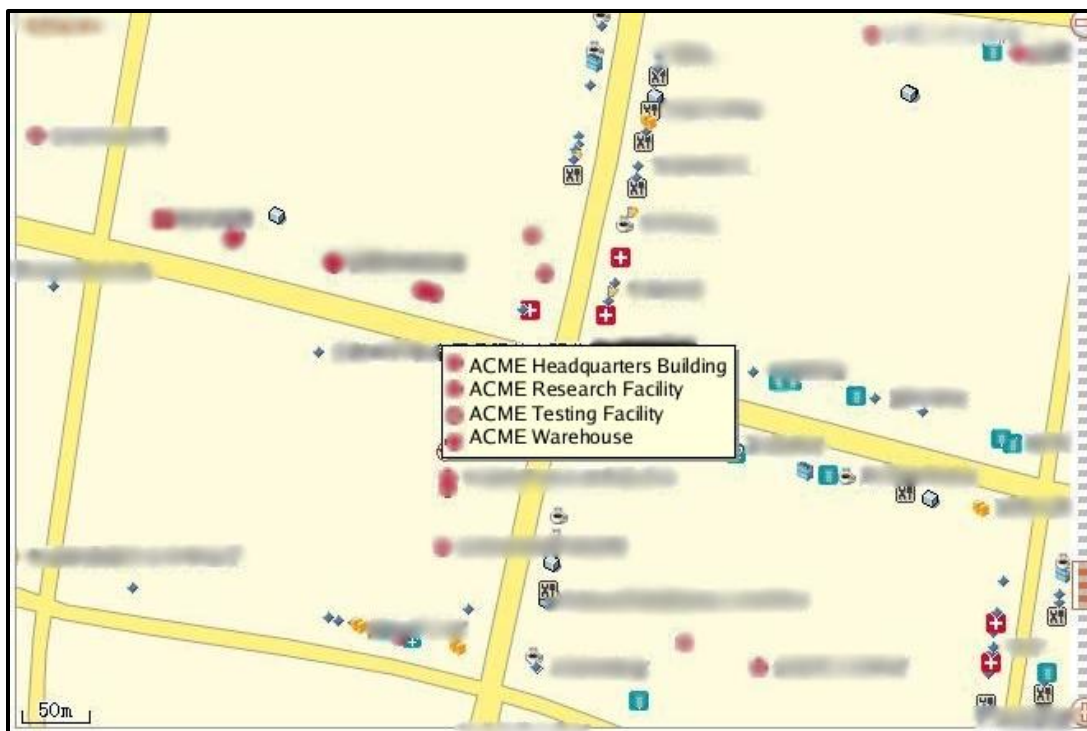
Example: Actor Dossier

Utilized non-satellite photos to located place of work on public satellite images of the city



Example: Actor Dossier

Country specific street maps identified that the building belonged to the overall organization in question, “ACME”



Person → Organization

TASK: *Research the actor “sn33kydvl” and determine any affiliation with “ACME”*

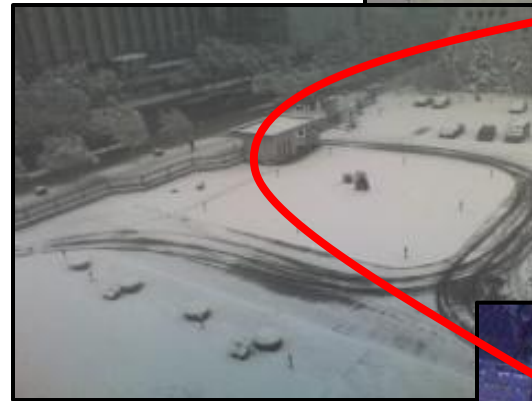
RESULTS:

- Found a personal blog which includes hacking information and photos from within and in front of their workplace
- Located this building on public satellite images of the city
- Country specific street map engine identified that this building belonged to the overall organization under question, “ACME”.

IMPACT:

- After years of research based on other methods, Internet Based Reconnaissance effectively linked “sn33kydvl” to the “ACME” organization within 3 weeks

Standing in front of offices



View from inside building



Satellite Image and Street Map



Profiling Individuals

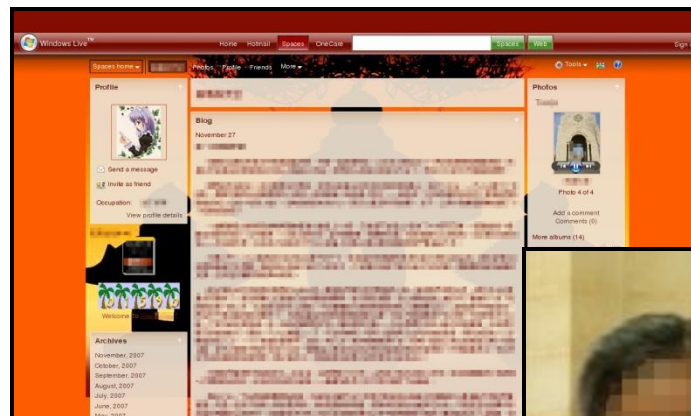
TASK: Find true identity of “icejane56”

RESULTS:

- Discovered a personal blog and forum postings discussing travel to a conference on a specific date, in a specific city, and the time they were speaking at the conference
- Found email address and pictures of this actor linking them to an organization
- Identified the exact conference, schedule, and all speakers and paper contributors
- Identified 4 speakers, from the same university, speaking at the stated time, and researched each until only one remained; *Sue Jane Smith* (the only female)

IMPACT:

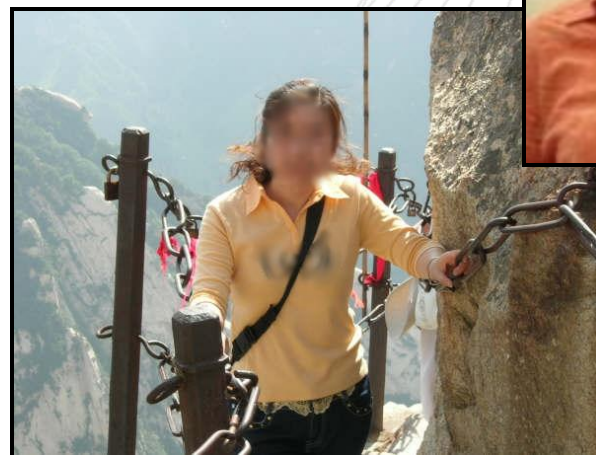
- Discovered true identity of “icejane56”, with pictures, and linked her to a specific department within the organization



Blog site



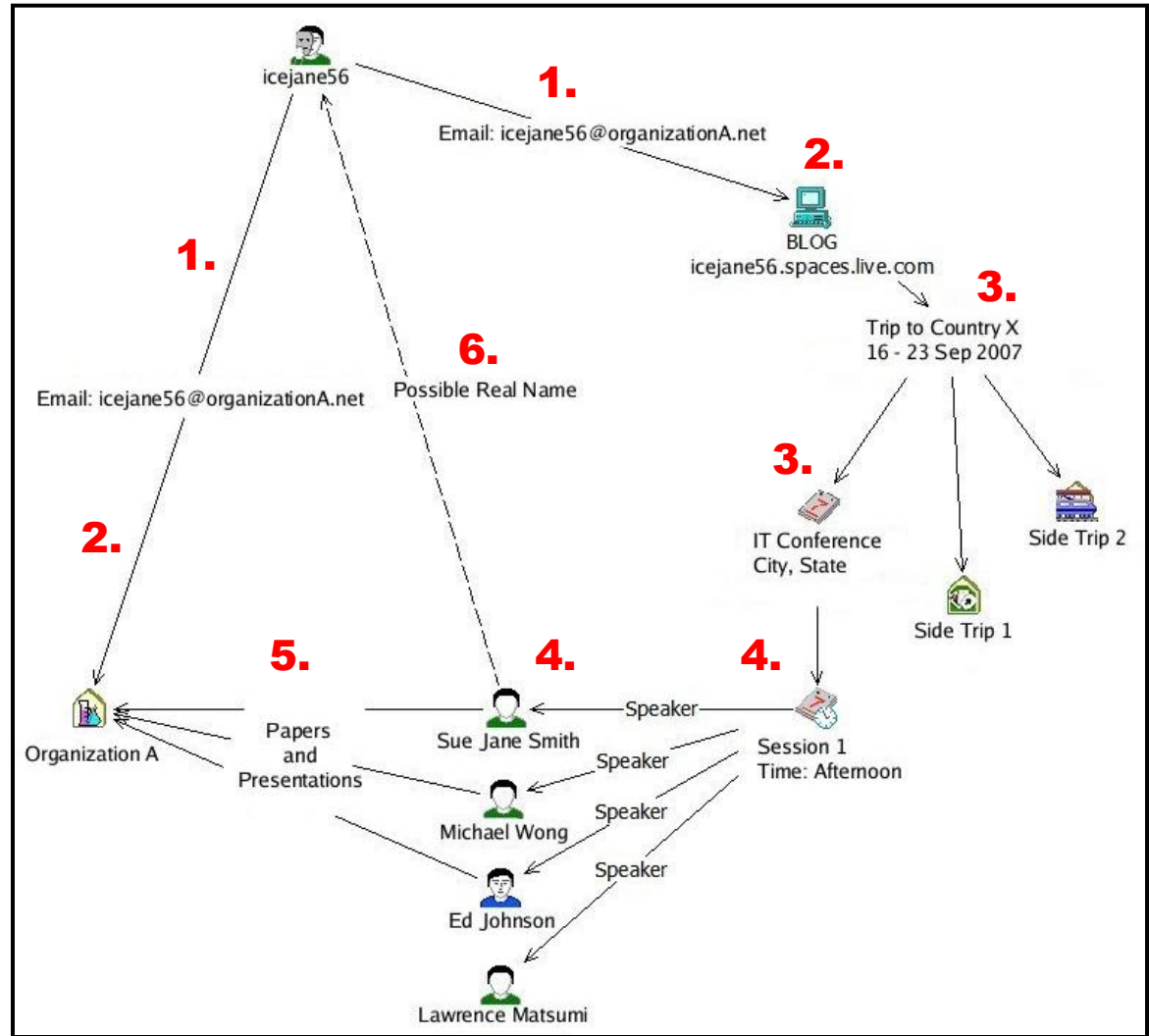
Personal Photographs of travels



Profiling Individuals: Association Diagrams

Created association diagram linking:

1. "icejane56" to an email
2. Email to Organization and blog
3. Blog to foreign trip and IT conference
4. Conference schedule to speaker names
5. Speaker names to Organization
6. One speaker was linked to the alias "icejane56"



Non-Satellite Photography

TASK: *Locate non-satellite photography of this entities location(s)*

RESULTS:

- Identified 4 distinct locations in the same city; Provided Lat/Long coordinates of each
- Found forum postings giving exact location of each, with road maps, along with pictures of the campus
- Matched each picture to a specific area within each location and marked each on satellite overview maps

IMPACT:

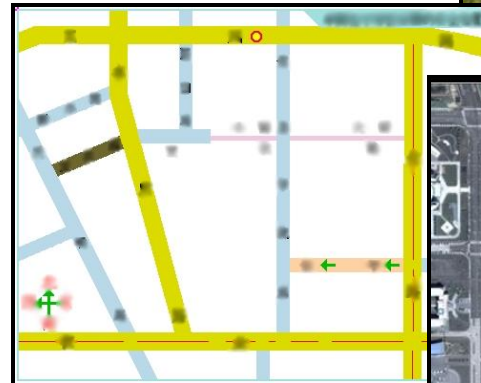
- Provided insight of layout and building structure of each location, and identified specific purpose of many buildings



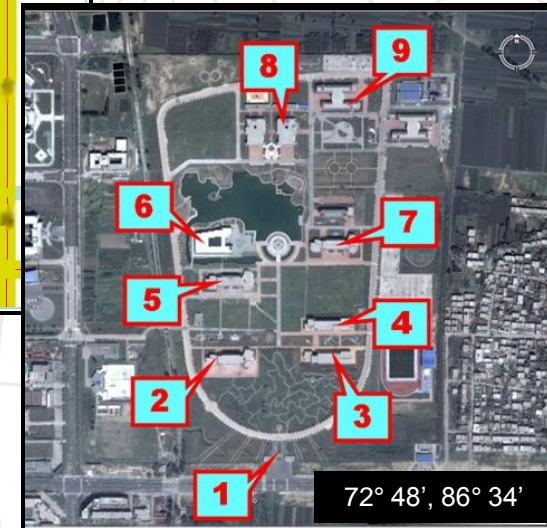
Main Entrance



Dining Hall



Street map
&
Annotated
Satellite Image



Geographically Locating Entities

TASK: Find entity from country A within a city in country B

RESULTS:

- Discovered phone number for entity
- Identified only phone company to service the area and was able to retrieve last phone bill, using the phone number, which listed current address in local native language
- Utilized current and historical maps to locate exact location and identified adjacent businesses to entity
- Identified key personnel within building

IMPACT:

- Confirmed exact location of entity, and profiled surrounding area



1. Foreign Offices 1
2. Airline Office
3. ACME Bank
6. Entity A Offices
7. Foreign Offices 2
8. Foreign Offices 3
10. Residential Apts
11. Clothing Store
12. School
16. Local Bank
17. Trading Company

Annotated Satellite Map

Customer Information		Phone Number : 123-456-7890	Phone Class :	Not Residential	Display Date: 8/12/2006 at 04:24					
Local Bill(s)										
Invoice Date : 01/10/2006										
Subscriber Name : Some place			Consumption : From 01/05/2006 To 31/07/2006							
Subscription	Extra Calls	National	Trunk (18)	Audio	Insurance	Previous Balance	Stamps	Free Internet	Package Subscription	
48.00	4.48	0.01	0.00	0.00	0.00	0.00	0.00	5.00	0.00	
Package Discount	Features	Internet	Mobile	Photograph (10)	Free Number	Admin Fees	Delays	Sales Tax	Commercial Tax	
0.00	0.00	0.00	0.90	0.00	0.00	0.00	0.00	5.73	0.00	
Sub-Total excluding stamps and sales tax			59.22	Total Amount ()		64.95				
Invoice Date : 01/07/2006										
Subscriber Name : Some place			Consumption : From 01/02/2006 To 30/04/2006							
Subscription	Extra Calls	National	Trunk (18)	Audio	Insurance	Previous Balance	Stamps	Free Internet	Package Subscription	
48.00	3.03	0.01	0.00	0.00	0.00	0.00	0.40	0.00	0.00	
Package Discount	Features	Internet	Mobile	Photograph (10)	Free Number	Admin Fees	Delays	Sales Tax	Commercial Tax	
0.00	0.00	0.00	0.91	0.00	0.00	0.00	0.00	5.13	0.00	
Sub-Total excluding stamps and sales tax			52.92	Total Amount ()		58.45				
International Bill(s)										
For month	Calls	Duration (min)	Calls Amount	Stamps	Sales Tax	Overseas	Profit Tax ()	Admin Fees	Total Amount	Due Date
01/10/2006	5	12	0.50	0.00	4.35	0.00	0.00	0.00	45.85	10/12/2006
01/09/2006	15	30	06.10	0.00	9.61	0.00	0.00	0.00	105.75	10/12/2006
View Previous Local Bills						View Previous International Bills				
Summary										
ePay		Bill Description	Amount	Admin Fees and Taxes	Total					
Paid via central on 24/09/2006		Local Bill 01/10/2006	59.22	0.00	64.95					
Paid via central on 28/08/2006		Local Bill 01/07/2006	52.92	0.00	59.45					
Paid via central on 05/12/2006		International Bills 01/10/2006	46.85	0.00	46.85					
Paid via central on 02/11/2006		International Bills 01/09/2006	105.75	0.00	105.75					
			Total Due ()							
You can add another invoices for more than one phone number, you can save all the selected invoices by click on button (Add Invoice For Payment)										
										<input type="button" value="Add Invoice For Payment"/> <input type="button" value="ePay"/> <input type="button" value="Close"/>

Retrieved Phone Bill

Network Enumeration Capability

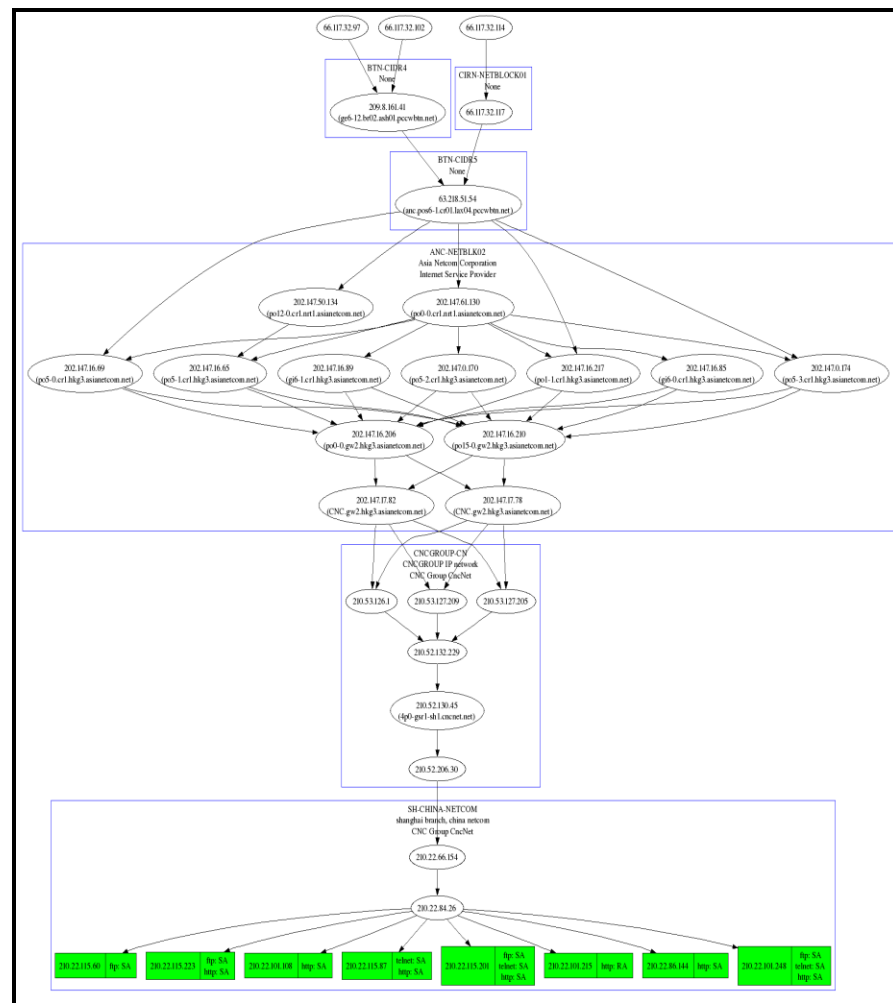
TASK: *Enumerate remote networks to identify open ports and network architecture*

RESULTS:

- Enumeration results return open ports, banner text, operating systems, and network applications in use
- Enhanced traceroutes utilize results from above to provide graphical view of traffic flow into the network, and also provides network owner and hostname information for discovered nodes/networks

IMPACT:

- Identifies potential weaknesses of remote network and hierarchical view of network architecture



Enhanced Graphical Traceroute



Network Enumeration with Open Source Research

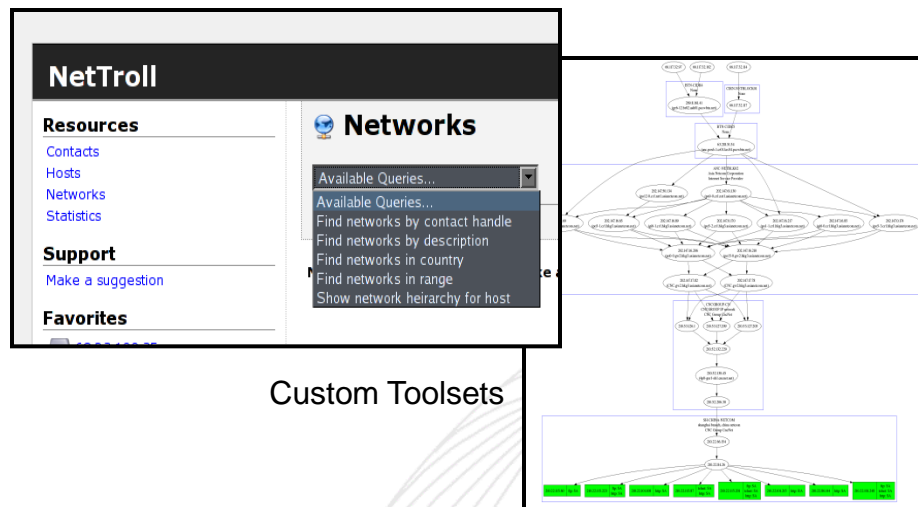
TASK: *Identify hardware / software in a specific remote IP network*

RESULTS:

- Custom toolsets provided all port, banner, and hostname information and enhanced traceroutes provided diagram
- Found posted announcements at multiple sites of hardware upgrades/purchases for the associated network
- Correlated the hostname/banner data with the announcements to identify exact models of hardware in use, and where they are in the network

IMPACT:

- Identified specific hardware within the network and existing vulnerabilities



NetTroll

Resources
[Contacts](#)
[Hosts](#)
[Networks](#)
[Statistics](#)

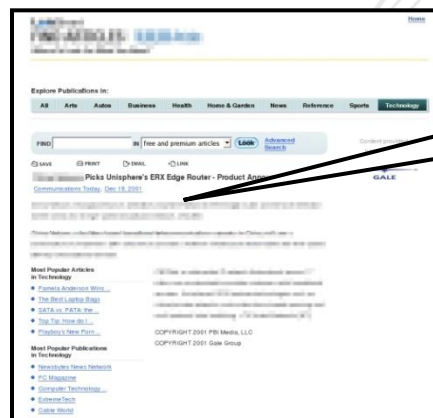
Support
[Make a suggestion](#)

Favorites

Networks

Available Queries...
 Find networks by contact handle
 Find networks by description
 Find networks in country
 Find networks in range
 Show network heirarchy for host

Custom Toolsets



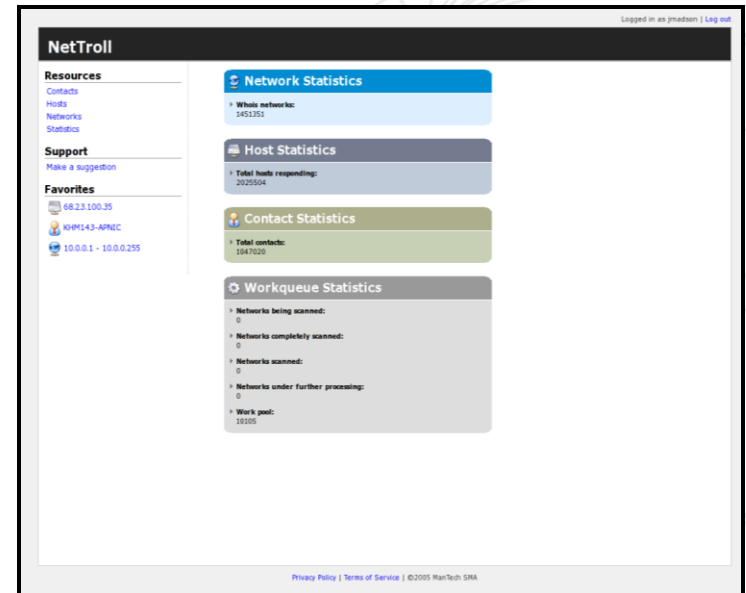
ACME recently upgraded all their edge routers to Juniper ERX-9002si's.

Open Source Research



NetTroll: One of our Custom Tools available to You!

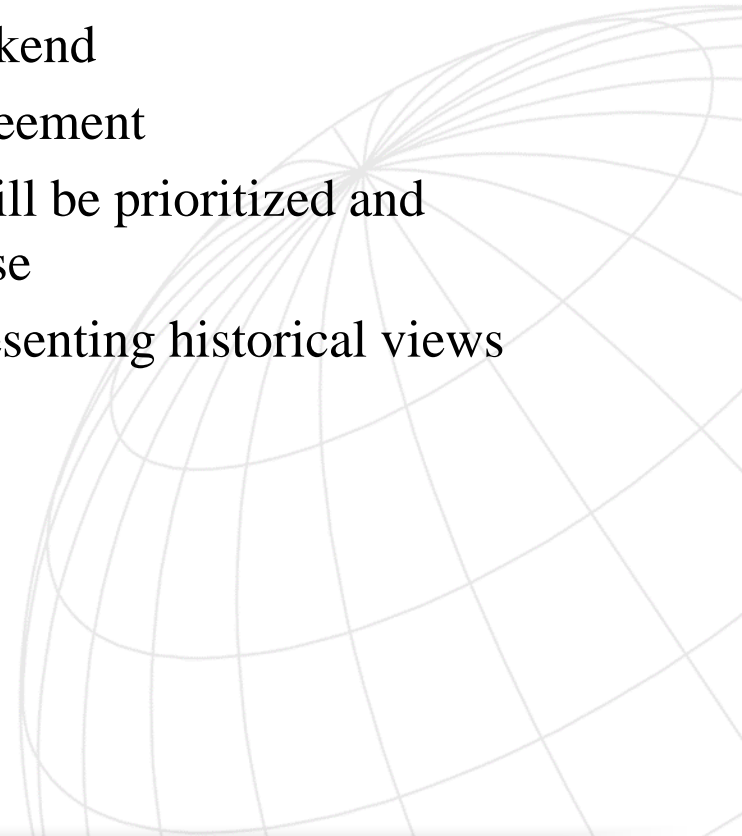
- Searchable database of Internet host and network information
- Combines open source collection data
- Shows
 - Host operating system information per port
 - Open/closed ports with banners
 - Correlated network and domain registration information
- Numerous available searches
 - IP, Network, Range, Country
 - Person, email address
 - Service banner keyword
 - Data correlation



NetTroll HomePage

NetTroll Features

- Ability to bookmark favorite views for quick reference
- Data may be exported in CSV format
- Secure web interface with robust database backend
- Supports multiple seats based on licensing agreement
- Ability to suggest online enhancements that will be prioritized and implemented to benefit entire IC/DoD user base
- Looking at adding routing information and presenting historical views



NetTroll Benefits

- Rapidly decreases information gathering timeline
- Decreases level of expertise and training needed to gather the data
- Eliminates infrastructure resources required to scan for the data (non-attrib lines, operators, operations center)
- Removes legal implications
 - You do not ask Google to scan all the web servers on the Internet ... the information is just available
 - Nor do you ask NetTroll to scan all the systems on the Internet ... the information is just available
- Provides fresh open source enumeration data at your fingertips

NetTroll Functionality

NetTroll

Resources

- [Contacts](#)
- [Hosts](#)
- [Networks](#)
- [Statistics](#)

Support

[Make a suggestion](#)

Favorites

Networks

Available Queries...

- Available Queries...
- Find networks by contact handle
- Find networks by description
- Find networks in country
- Find networks in range
- Show network heirarchy for host

Drop Down Queries




Resources

- [Contacts](#)
- [Hosts](#)
- [Networks](#)
- [Statistics](#)

Support

[Make a suggestion](#)

Favorites

-  68.23.100.35
-  KHM143-APNIC
-  10.0.0.1 - 10.0.0.255

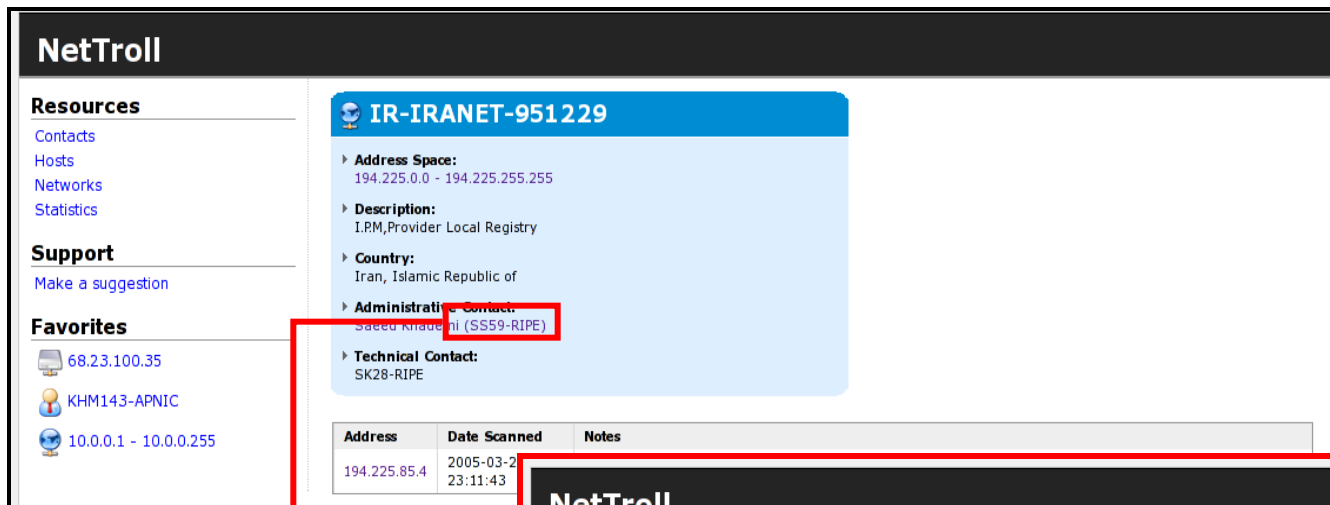
Networks

Find networks in country ▼

Country: Iran, Islamic Republic of ▼

Network Name	Address Range	Country	Description
ACDGROUPS	194.146.164.0 - 194.146.167.255	IR	Asia Communication Developers Group Co.
adakrayaneh	217.219.231.0 - 217.219.231.255	IR	isp.co
ADLDELFANNOOR	217.219.211.32 - 217.219.211.63	IR	Adl delfan Gostar nooranad ,Internet Service Provider
AEOI	80.191.7.208 - 80.191.7.223	IR	Atomic Energy Organization of Iran
Afganistan	213.155.61.128 - 213.155.61.255	IR	afganistan
afra	217.11.16.0 - 217.11.16.255	ir	AFR@NET company, Tehran, Iran,E1 lines
AFRACOSHIRAZ	217.219.101.128 - 217.219.101.159	IR	Afra co.,Internet service provider
afranet	217.218.98.0 - 217.218.98.255	IR	Afranet Co
Afroz	217.218.83.96 - 217.218.83.111	IR	Afroz Network Solutions,provide Dialup and Wireless Internet access
Afroz-NET	81.12.45.0 - 81.12.45.255	IR	Afroz Network Solutions,provide Dialup and Wireless Internet access
AFTAB	62.193.9.0 - 62.193.9.255	IR	AFTAB Co.(ISP)- Data Processing Of Iran
Aftab-20041120	81.12.66.0 - 81.12.66.255	IR	Aftab Communications & Informatics , INC.
AFTAB-TGB	195.219.50.0 - 195.219.50.255	IR	AFTAB Co.(ISP)- Data Processing Of Iran
AftabCo	62.145.82.0 - 62.145.82.255	IR	AftabCo (IMS Customer)
aftabomahtab	217.218.228.128 - 217.218.228.255	IR	isp.co.
AFTABRAYAN	217.219.28.160 - 217.219.28.255	IR	aftab rayane co. isb
AzareAsreNovin	217.11.17.32 - 217.11.17.63	Ir	developing specific hardware and required software to work together to help novice users work with computer easily
AGAHSZAJONOB	217.219.255.144 - 217.219.255.159	IR	Agahsaz jonoob Company ,Internet Service Provider
agh-ostan	217.219.147.192 - 217.219.147.207	IR	west azarbayjan province government
AGHDASIEH-POP	81.28.40.0 - 81.28.40.255	IR	Institute Isiran Aghdasieh POP,Internet Access Provider,provider LIR

NetTroll Functionality



NetTroll

Resources

- Contacts
- Hosts
- Networks
- Statistics

Support

[Make a suggestion](#)

Favorites

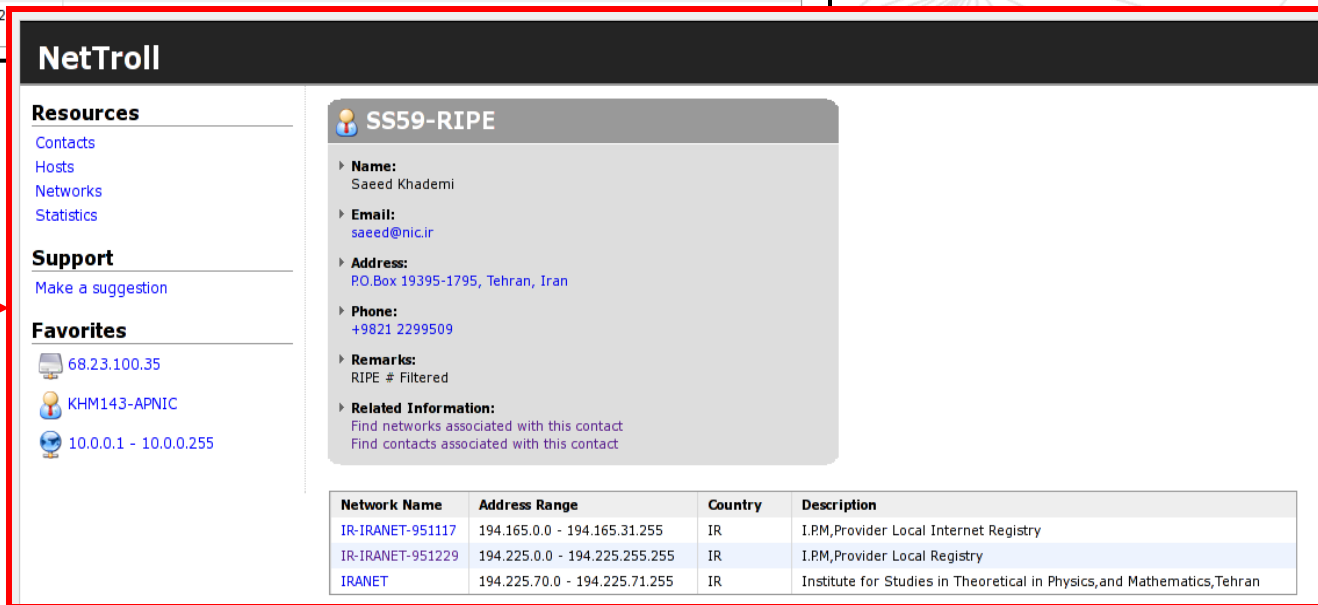
- 68.23.100.35
- KHM143-APNIC
- 10.0.0.1 - 10.0.0.255

IR-IRANET-951229

- Address Space:** 194.225.0.0 - 194.225.255.255
- Description:** I.P.M,Provider Local Registry
- Country:** Iran, Islamic Republic of
- Administrative Contact:** Saeed Khademi (SS59-RIPE)
- Technical Contact:** SK28-RIPE

Address	Date Scanned	Notes
194.225.85.4	2005-03-23:11:43	

Click to perform more extensive lookup of linked items



NetTroll

Resources

- Contacts
- Hosts
- Networks
- Statistics

Support

[Make a suggestion](#)

Favorites

- 68.23.100.35
- KHM143-APNIC
- 10.0.0.1 - 10.0.0.255

SS59-RIPE

- Name:** Saeed Khademi
- Email:** saeed@nic.ir
- Address:** P.O.Box 19395-1795, Tehran, Iran
- Phone:** +9821 2299509
- Remarks:** RIPE # Filtered
- Related Information:**
 - Find networks associated with this contact
 - Find contacts associated with this contact

Network Name	Address Range	Country	Description
IR-IRANET-951117	194.165.0.0 - 194.165.31.255	IR	I.P.M,Provider Local Internet Registry
IR-IRANET-951229	194.225.0.0 - 194.225.255.255	IR	I.P.M,Provider Local Registry
IRANET	194.225.70.0 - 194.225.71.255	IR	Institute for Studies in Theoretical in Physics,and Mathematics,Tehran

NetTroll Functionality

NetTroll




Resources


- [Contacts](#)
- [Hosts](#)
- [Networks](#)
- [Statistics](#)

Support

[Make a suggestion](#)

Favorites


-  [68.23.100.35](#)
-  [KHM143-APNIC](#)
-  [10.0.0.1 - 10.0.0.255](#)

 **IR-IRANET-951229**

- ▶ **Address Space:**
194.225.0.0 - 194.225.255.255
- ▶ **Description:**
I.P.M,Provider Local Registry
- ▶ **Country:**
Iran, Islamic Republic of
- ▶ **Administrative Contact:**
Saeed Khademi (SS59-RIPE)
- ▶ **Technical Contact:**
SK28-RIPE

Address	Date Scanned	Notes
194.225.85.4	2005-03-20 23:11:43	TCP MSS Option on port 22: 1460 response: 4:8:18 GMT ICMP Port

Click to perform more extensive lookup of linked items

 **194.225.85.4**

- ▶ **Network:**
[IR-IRANET-951229](#)
- ▶ **Reverse Address:**
- ▶ **Country:**
Iran, Islamic Republic of
- ▶ **Scan Time:**
2005-03-20 23:11:43
- ▶ **Notes:**
TCP MSS Option on port 22: 1460 ICMP Port Unreach from interface: 194.225.85.5 ICMP Timestamp response: 4:8:18 GMT ICMP Port Unreach from interface: 194.225.85.5
- ▶ **Related Information:**
[Show network heirarchy for host](#)

Network Name	Address Range	Country	Description
IR-IRANET-951229	194.225.0.0 - 194.225.255.255	IR	I.P.M,Provider Local Registry
TED-NET	194.225.85.0 - 194.225.85.255	IR	Primary Education Organization,Taleghani St., Felestin Sq.,Tehran

page 1 of 1
2 results | export: [CSV](#)

Port	Status	Operating System	Banner
21	closed	Linux 2.2.x (90%)	
22	OPEN	Linux 2.2.x (95%)	SSH-2.0-OpenSSH_3.8.1p1 FreeBESL-20040419.

NetTroll Summary

- Searchable database of Internet host and network information
- Combines open source collection data
- Shows:
 - Host operating system information per port
 - Open/closed ports with banners
 - Correlated network and domain registration information



Internet-based Reconnaissance Operations Summary

- Non-attributable open source research using
 - Customized tools such as NetTroll
 - To analyze both internal and external internet presences
 - Whether they are:
 - People
 - Places
 - Networks
 - Technologies

