# NicLabs
# NIC Chile's Research Laboratory

Tomás Barros

Reseco Workshop, Santiago November 25th, 2008

NIC CHILE Research labs

# NicLabs

- New Research Laboratory Held by NIC Chile (TLD of the .CL zone)
- Created on 2008
- Its mission is to develop Internet in Chile by producing world class apply research around IP technologies.
  - Generating new knowledge and sharing it with the community.
  - Doing technology transfer
  - Becoming a national reference about Internet Technologies.

NIC CHILE Research labs

# NicLabs Methodology

Based on Specific Projects

- Required by NIC
  - DNS Analysis and research
  - Technical concerns
- Required by or proposed to enterprises/Government
  - ENTEL PCS
  - SixLabs
  - Asociación de Proveedores de Internet (API)
  - Subsecretaría de Telecomunicaciones
  - Codelco
  - SkillUp Japan
  - NovaWare USA
- In Collaboration with the International Scientific Community

NIC CHILE Research labs

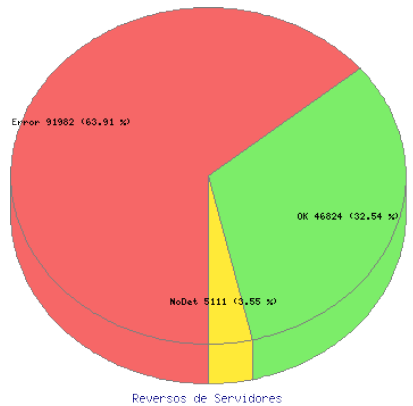
# DNS Analysis and research

## Active analysis

### .CL Pulsómetro


| Nombre | Tipo | Evaluación OK | No Determinada | Evaluación Error | Comparación |
|---|---|---|---|---|---|
| Servidores Activos | N | 105351 (73.20 %) | 38566 (26.80 %) | 0 (0.00 %) | |
| Reversos de Servidores | N | 46824 (32.54 %) | 5111 (3.55 %) | 91982 (63.91 %) | |
| Respuesta con Autoridad | N | 101276 (70.37 %) | 38566 (26.80 %) | 4075 (2.83 %) | |
| Análisis de CNAME para NS | N | 105137 (73.05 %) | 38566 (26.80 %) | 214 (0.15 %) | |
| MX es nombre de HOST | N | 92944 (64.58 %) | 41715 (28.99 %) | 9256 (6.43 %) | |
| Reverso de MX | N | 14348 (9.97 %) | 50523 (35.11 %) | 79044 (54.92 %) | |
| Completitud de Servidores | R | 57982 (40.29 %) | 0 (0.00 %) | 85935 (59.71 %) | |
| Número de servidores | R | 133951 (93.08 %) | 0 (0.00 %) | 9966 (6.92 %) | |
| Recursividad | R | 75638 (52.56 %) | 38566 (26.80 %) | 29713 (20.65 %) | |
| Clases de direcciones IP | R | 70986 (49.32 %) | 0 (0.00 %) | 72931 (50.68 %) | |
| Versiones de Software DNS | R | 52077 (36.19 %) | 46237 (32.13 %) | 45603 (31.69 %) | |
| Número Serial | R | 113283 (78.71 %) | 28935 (20.11 %) | 1698 (1.18 %) | |
| Nombre Servidor Primario en SOA | R | 76988 (53.50 %) | 33989 (23.62 %) | 32939 (22.89 %) | |
| Formato Número Serial | R | 93559 (65.01 %) | 31602 (21.96 %) | 18755 (13.03 %) | |
| Tiempos del SOA | R | 62125 (43.17 %) | 33538 (23.30 %) | 48253 (33.53 %) | |
| Tiempo de Refresco | R | 16793 (11.67 %) | 38987 (27.09 %) | 88136 (61.24 %) | |
| Tiempo de Reintento | R | 109511 (76.09 %) | 29609 (20.57 %) | 4796 (3.33 %) | |
| Tiempo de Expiración | R | 18582 (12.91 %) | 38689 (26.88 %) | 86645 (60.21 %) | |
| TTL | R | 70168 (48.76 %) | 33583 (23.34 %) | 40165 (27.91 %) | |
| Registro WWW | R | 52780 (36.67 %) | 38566 (26.80 %) | 52570 (36.53 %) | |
| Registro MX | R | 82152 (57.08 %) | 52573 (36.53 %) | 9191 (6.39 %) | |
| CNAME para MX | R | 82103 (57.05 %) | 52573 (36.53 %) | 9240 (6.42 %) | |
| Número de registros MX | R | 10638 (7.39 %) | 51604 (35.86 %) | 81673 (56.75 %) | |

- 23 evaluations by zone
- National Statistical
- Evolution in time

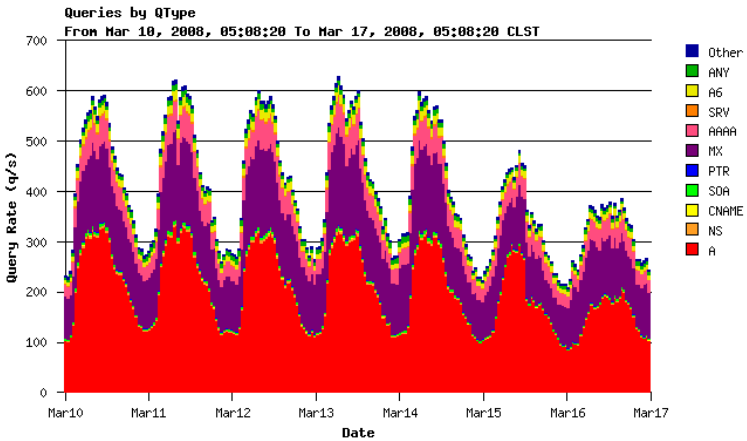


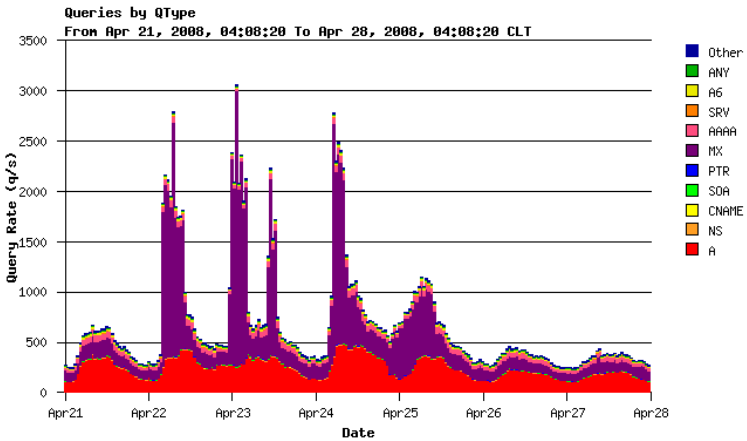

NIC CHILE Research labs

# DNS Analysis and research

## Passive analysis

### DNS queries characterisation



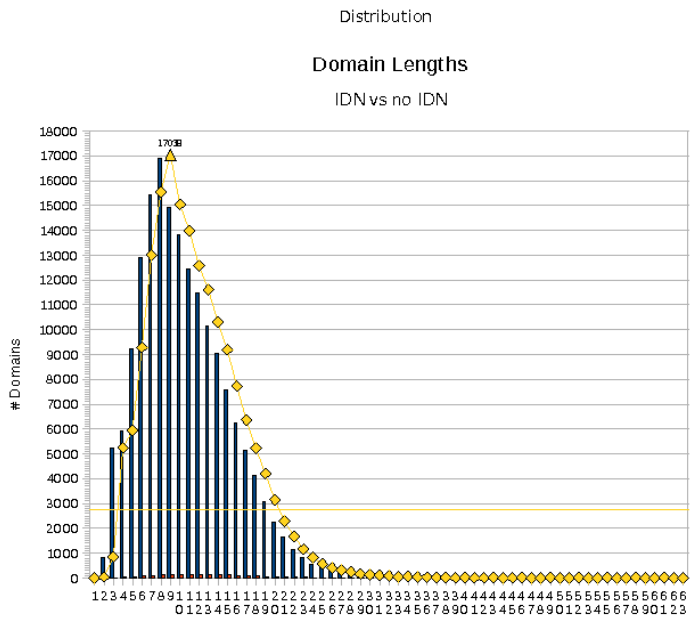



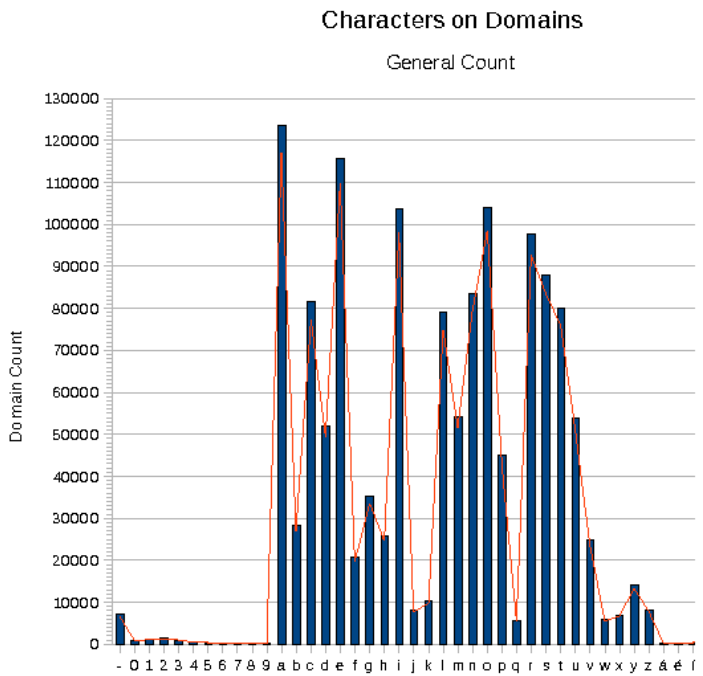
# DNS Analysis and research

## Passive analysis

### Domain registration characterisation

- Define Semantic groups
- Introduce an alternative to Levenshtein distance based on a membership relative to a specific dictionary
- Dictionaries built on periodically news



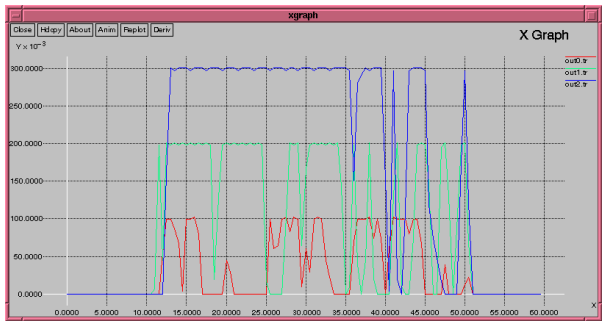



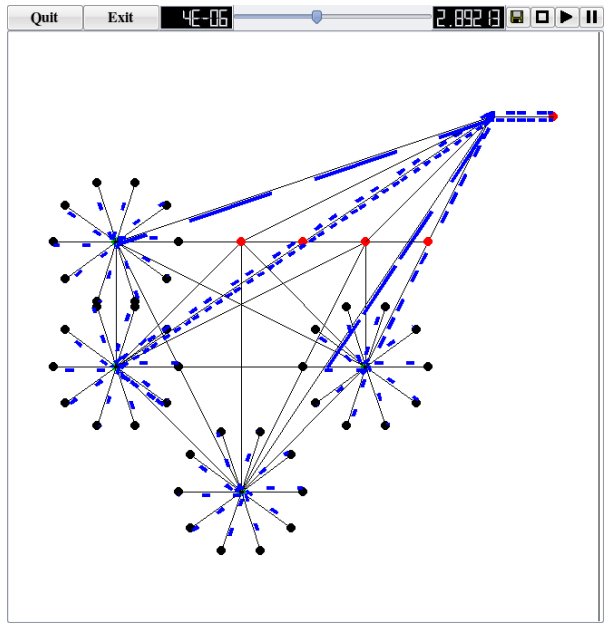

NIC CHILE Research labs

# DNS Analysis and research

## Simulations

- AnyCast Cloud versus Round Robin (or both)
- Validated with real experiments
- Use:
  - Stress and collapse analysis
  - Find optimal configurations



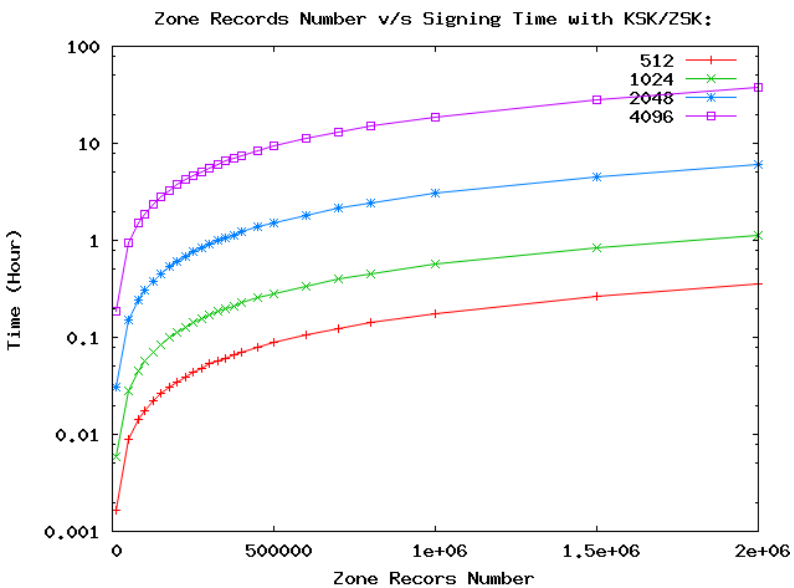



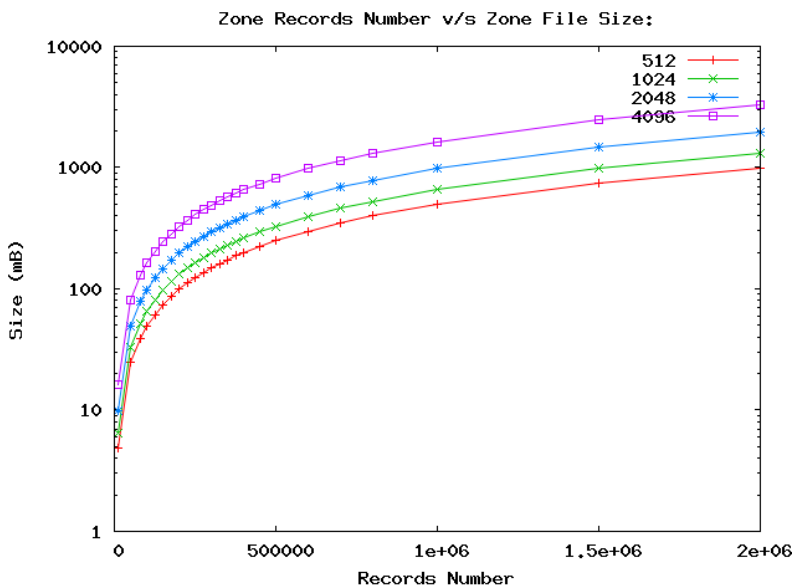

NIC CHILE Research labs

# Technical Concerns

## DNSSEC

- Impact on systems
- Impact on processes
- Provide clues to take decisions




NIC CHILE Research labs

# External projects

## ENTEL PCS

- Multimedia Streaming over 3G networks
- Localisation using antennas
- Linux driver for 3G modems
- DB analysis for scalability

NIC CHILE Research labs

# External projects

## SixLabs

- Definition and implementation of a Service Delivery Platform (SDP)
- IP version 6 support
- Innovation services
- Redundancy implementation
- Garbage Collector performance

NIC CHILE Research labs

# External projects

## Asociación de Proveedores de Internet (API)

- Chilean IPv6 Task Force
  - Diffusion and Training
  - IPv6 Bone
  - Apply Research
- Internet Security Agency

NIC CHILE Research labs

# External projects

## Subsecretaría de Telecomunicaciones

Number Portability for Chile

- Setting up the technical solution for Chile
- Introducing the regulation
- Coordinating with the operators
- Proposing extensions

NIC CHILE Research labs

# External projects

## SkillUp Japan

Content Smart Distribution
Distribution of content for heterogeneous devices and media transmission. Transport and signalling of H264/SVC over Stream Control Transmission Protocol (SCTP)

- Trade-off between quality and delay
- Real Implementation over 3G networks
- Simulation and analysis in NS2
- Firewall traversal
- Peer-to-peer using SCTP
- Peer-to-peer mesh construction

NIC CHILE Research labs

# External projects

## NovaWare USA

Remote Health Care

- Open health platform
- Wearable communicating devices
- Remote evaluation
- Continuous monitoring

NIC CHILE Research labs

# Scientific Collaboration

## France, Uruguay, Argentina, Brasil

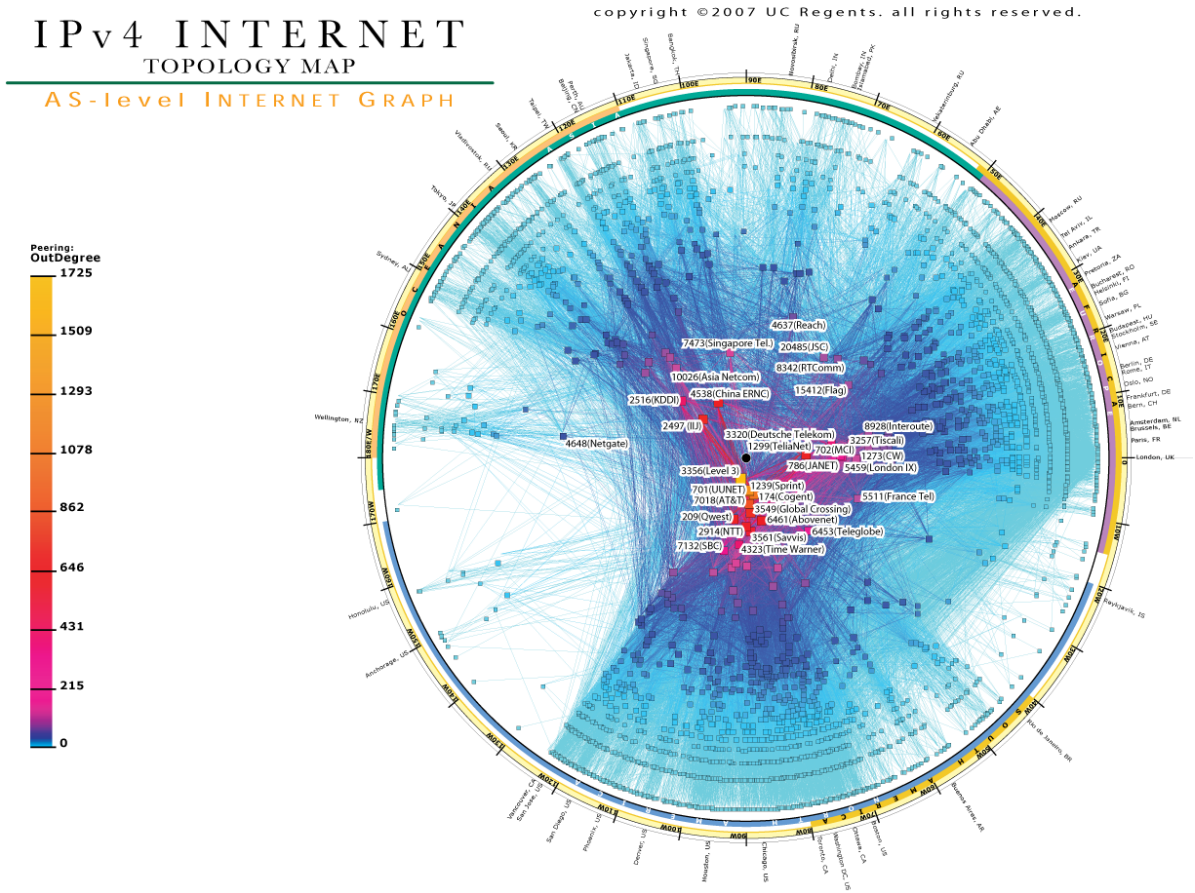
- ReSeCo: Reliability and Security of Distributed Software Components
- FMCrypto: Formal Methods for Cryptographically Secure Distributed Computations
- SCAN – Self-Conscious Ambient Networks

NIC CHILE Research labs

# Coming Next

## Active analysis

### Chilean Internet Map




NIC CHILE Research labs

# Coming Next

## Passive analysis

### Other analysis

- DNS Anomalies
  - SPAM [1]
  - Botnets Detection [2]
  - Final User Impact [3]


Bojan Zdrnja, Nevil Brownlee and Duane Wessels

Passive Monitoring of DNS Anomalies

Detection of Intrusions and Malware, and Vulnerability Assessment, LNCS 4579, 2007.

John Kristoff

Botnets, detection and mitigation: DNS-based techniques

Information Security Day, Northwestern University, July, 2005.

Anees Shaikh, Renu Tewari, and Mukesh Agrawal

On the Effectiveness of DNS-based Server Selection

In Proceedings of IEEE INFOCOM 2001, Anchorage, Alaska.


NIC CHILE Research labs

# Coming Next

## Technical Concerns

- IPv6
- ENUM

NIC CHILE Research labs

# Eventually

## Other Projects

- Open-Source software/systems
- Atomisation and sensors
- Low cost and good quality National Internet access

NIC CHILE Research labs

# NicLabs

## The Team

- 3 Researchers
- 4 Master Students
- 4 Engineers
- 1 Under graduate student
- Several Collaborations

NIC CHILE Research labs

# Collaborations

## ReSeCo and FMCrypto

what we can do together ?

NIC CHILE Research labs

# Collaborations

## ReSeCo and FMCrypto

what we can do together ?

- Create a formal method branch within NicLabs

NIC CHILE Research labs

# Collaborations

## ReSeCo and FMCrypto

what we can do together ?

- Create a formal method branch within NicLabs
- Formalisation of DNS/DNSSEC

NIC CHILE Research labs

# Collaborations

## ReSeCo and FMCrypto

what we can do together ?

- Create a formal method branch within NicLabs
- Formalisation of DNS/DNSSEC
- Open source system for e-voting

NIC CHILE Research labs

# Collaborations

## ReSeCo and FMCrypto

what we can do together ?

- Create a formal method branch within NicLabs
- Formalisation of DNS/DNSSEC
- Open source system for e-voting
- Strong authentication using mobile devices

NIC CHILE Research labs

# Collaborations

## ReSeCo and FMCrypto

what we can do together ?

- Create a formal method branch within NicLabs
- Formalisation of DNS/DNSSEC
- Open source system for e-voting
- Strong authentication using mobile devices
- Distributed Internet data collector for final users... proof of concept for secure distribution

NIC CHILE Research labs

# Collaborations

## ReSeCo and FMCrypto

what we can do together ?

- Create a formal method branch within NicLabs
- Formalisation of DNS/DNSSEC
- Open source system for e-voting
- Strong authentication using mobile devices
- Distributed Internet data collector for final users... proof of concept for secure distribution
- Any suggestion is welcome!

NIC CHILE Research labs