



Double Shot Security and APNIC Training

Infrastructure and service provider security
tutorial

12th August 2008, SANOG12
Kathmandu, Nepal

SANOG

Introduction

Presenters

- Merike Kaeo
CEO, Double Shot Security
- Miwa Fujii
APNIC Training Officer, Research and Development
<miwa@apnic.net>

Agenda

- Internet security status quo
- Identifying attackers – hiding addresses and tracing miscreants
- Anatomy Botnets, DNS hijack and etc.
- APNIC whois database
- Digital forensics overview
- Attack detection techniques, forensic and mitigation tools for ISPs

Scope

- To provide wide and general information about current issues related to cyber attacks and forensics
- To enhance awareness of importance of network security and each organisation's responsibilities
- To provide a starting point for developing a forensic capability
- To provide above information from an IT point of view, not a law enforcement view

Outside of scope

- Each organisation operates under different law and regulations, it is NOT scope of this presentation:
 - to provide tangible guidelines
 - to execute a digital forensic investigation
 - to provide legal advice
 - nor to provide a basis for investigations of criminal activities.
- Describing technical details of specific network forensics processes

Note

- Certain commercial organisations and their products and services may be mentioned in this module. However such identification does not imply recommendation or endorsement by APNIC nor organisations and authors that APNIC referred to develop this module.

Acknowledgement

- This material refers many research outcomes provided by various organisations such as Arbor, Symatec and SANS Internet Storm Centre.

Internet security status quo

The Storm Worm

- 15 Jan 2007, an innocuous looking email was sent to many computers in the world
- The subject line said “230 dead as storm batters Europe”
- Actually, a big storm hit northern Europe at around the same time
- The email contained a file attached with plausible-sounding name. Example for:
 - FullStory.exe
 - Read More.exe
- Trojan!
 - infecting something like a million computers worldwide
 - still out there
- The Trojan was distributed that opens up a back door that can be exploited later on

At that time, huge storms sweep northern Europe

BBC NEWS | Europe | Huge storms sweep northern Europe - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://news.bbc.co.uk/2/hi/europe/6274377.stm

January 2007 storm in Europe

BBC NEWS | Europe | Huge storm... ent-whitepaper_internet_security_thr... Logon - Version 9.3.02 "Innocuous"の検索結果(18件) - 英辞...

Home News Sport Radio TV Weather Languages Search

UK version International version About the versions Low graphics Accessibility help

BBC NEWS WATCH One-Minute World News News services Your news when you want it

News Front Page Last Updated: Thursday, 18 January 2007, 22:34 GMT E-mail this to a friend Printable version

Huge storms sweep northern Europe

At least 25 people have been killed as violent storms lashed northern Europe, causing travel chaos across the region.

Britain was the worst hit with nine people killed as rain and gusts of up to 99mph (159km/h) swept the country.

Hurricane-force winds battering Germany have claimed at least seven lives. The other deaths were reported in France, the Czech Republic and the Netherlands.

The severe weather has forced hundreds of flight, rail and ferry cancellations and prompted road and school closures.

Meteorologists at London's Met Office said the winds reached "severe gale force" as they crossed Britain and were the highest recorded since January 1990.

They warned the weather system would intensify as it moved east across the continent - with Denmark, the Netherlands and Germany expected to be worst hit overnight.

Winds of almost 105mph (170km/h) were recorded late on Thursday in Germany, prompting the national rail company to suspend all its services, leaving passengers stranded.

The head of German railways said the situation was unprecedented. Air traffic too has been badly affected with many flights cancelled. There

Huge waves pound the port of Wimereux, northern France

WATCH Aftermath of storms

SEE ALSO

- In pictures: Storms lash Europe 18 Jan 07 | In Pictures
- US harsh weather extends its grip 18 Jan 07 | Americas
- Rescue as ship sinks off Lizard 18 Jan 07 | Cornwall

TOP EUROPE STORIES

- EU treaty 'same as Constitution'
- Sarkozy to meet Putin in Moscow
- Georgian ex-minister 'confesses'

News feeds

MOST POPULAR STORIES NOW

MOST E-MAILED MOST READ

- Man in coma after mosquito bite
- Internet names for Asia launched
- Sculptor fills Tate with a hole
- UK warns Darfur rebels on boycott
- Burmese junta appoints go-between

Most popular now, in detail

STORM DEATHS

- Britain: 9
- Germany: 7
- The Netherlands: 4

Done DWL: 21.02%

start Microsoft PowerPoint ... BBC NEWS | Europe | ... EN 4:52 PM

http://news.bbc.co.uk/2/hi/europe/6274377.stm

A marvel of social engineering

- “The storm is a marvel of social engineering.”
- “Its subject line changes constantly.”
“...constantly changing its size and tactics to evade virus filters...”
 - Its subject line appeals human nature
 - Shock - “230 dead as storm batters Europe”
 - Outrage – “A killer at 11, he’s free at 21”
 - Prurience – “Naked teens attack home director”
 - Romance – “You asked me why”
 - Thus many people unconsciously allowed to invite the Trojan to their computer

Trojan + social engineering + organised crime

- The likely intention is to create many zombie computers:
 - To steal information
 - To further propagate large-scale spam and phishing runs
- “Trojan assaults of this scale are an unfortunate and increasingly common event. What is significant here though is the timely nature of this assault in relation to the European storm. Malware gangs are clearly using every technique and even tragedies like these to gain access to vulnerable machine”
 - By Mikko Hypponen, Chief Research Officer at F-Secure – among the first to detect the worm and named it as “The Storm Worm”

Even a worm can have a conscience?

- It appears that bad guys been pulling their punches
- “We’re lucky: so far they haven’t gone in for more lucrative damaging activities like online gambling, stock scams and stealing passwords and credit-card information”

Time October 8, 2007 p48

<http://www.time.com/time/magazine/article/0,9171,1666279,00.html>

- The Internet security is in limbo situation with bad guys’ mercy?

Time October 8, 2007 p48

<http://www.time.com/time/magazine/article/0,9171,1666279,00.html>

Some research results

ARBOR Worldwide Infrastructure Security
Report

Report by ARBOR

- Worldwide Infrastructure Security Report
 - Seventy self-classified Tier 1, Tier 2 and other IP network operators from North America, South America, Europe and Asia participated
 - Covering a 12 month period from July 2006 through July 2007
 - Volume III, published in September 2007
 - Available from:
 - <http://www.arbornetworks.com/report>

Some research results

Symantec Internet Security Threat Report

Report by Symantec

- Symantec Internet Security Threat Report
 - Trends for July – December 07
 - Volume XII, published April 2008
 - Available from
 - <http://www.symantec.com/business/theme.jsp?themeid=threatreport>
 - Symantec Internet Security Threat Report
 - Trends for July – December 07
 - Symantec Global Internet Security Threat Report
 - Trends for July – December 07

Identifying attackers

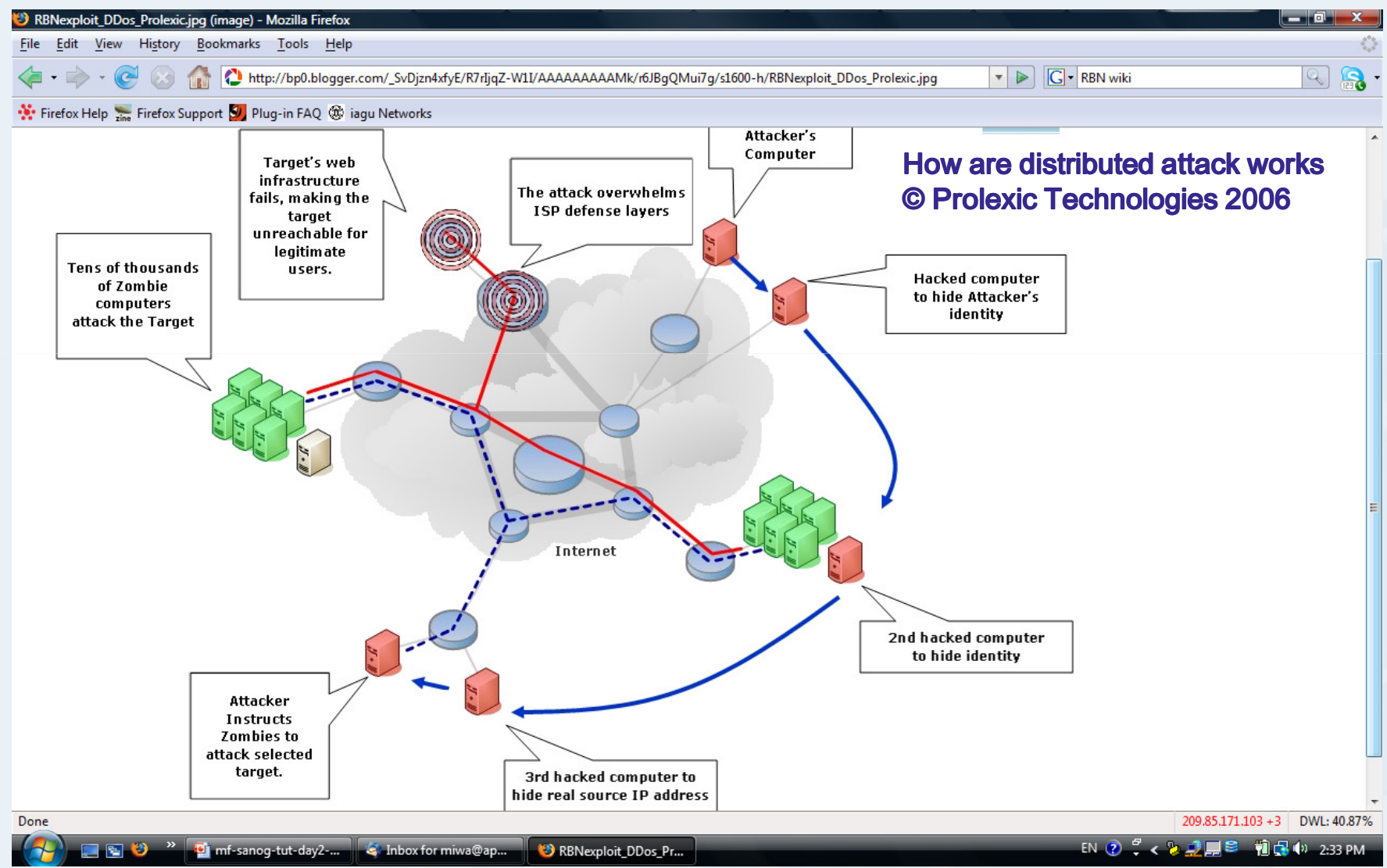
Identifying attackers

- Use Whois database
 - If you got a valid IP address of the attacker then you can use Whois database to track down the user of the address (theoretically)
 - We will cover this topic later in more details
- Seek ISP's help
 - If attacks is caused by forged IP addresses, this may provide some help
- Research the history of the IP address
- Look for clues in application content

Identifying attackers

- Identifying the IP address used by the attackers is unfortunately often not so easy and simple with various reasons:
 - IP address spoofing
 - Attackers to create IP packets with a forged (spoofed) source IP address with the purpose of concealing the identify of the attacker (the sender) or impersonating another computing system (Ref: http://en.wikipedia.org/wiki/IP_address_spoofing)
 - Numerous source IP addresses used by an attacker
 - Attackers can use fake IP addresses
 - Attackers can use BOTNET attack to compromise many computers to launch DDoS (Distributed Denial of Service) attack
 - IP address can be assigned dynamically
 - Use of DHCP in networks
 - Private IP address + NAT (Network Address Translator)

Hiding identities – example



And some people help to hide IP addresses



Ninja Surfing

Home Download Purchase Support About

Hide Your IP Address with Ninja Surfing for \$24.95!

Your current IP address is: **202.12.29.172**. Your computer located in: **Australia** . Be careful - IP address is a unique ID which points exactly to your location, with very high precision, right to the door of your apartment. 8-days free trial is available.

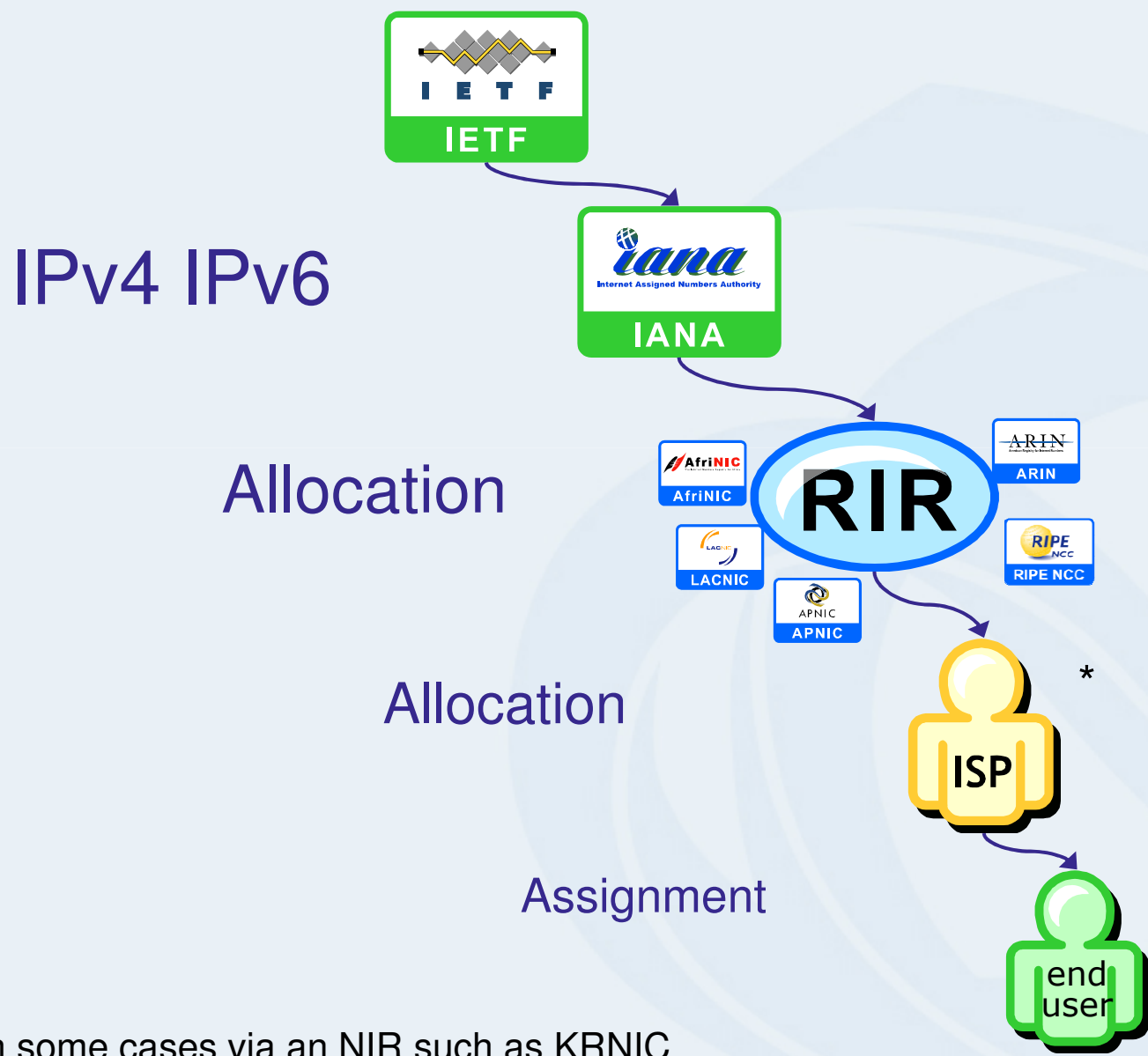
[Download Now](#) [Buy Now](#)

- **Hide IP address** - for completely anonymous web surfing.
- **Fake country of origin** - set your fake location to other country, surf anonymously and bypass restrictions enforced by some web sites.
- **Make anonymous forum posts** - and don't care - you can't be tracked.
- **Post messages to forums and newsgroups even when banned** - forum admin illegally banned you? Calm down, here is your solution.
- **Send e-mails anonymously** - never mind - you can't be detected by originator IP address.
- **Make secure purchases** - from restricted countries while travelling abroad.
- **Bypass content filtering** - enforced by government and ISP (read news, watch movies etc).
- **Access restricted sites** - bypass most ISP restrictions.

Copyright (C) 2006 Global Media, Inc. All rights reserved. | [Hide IP](#) | Email: support@NinjaSurfing.com

<http://www.ninjasurfing.com/>

So where do IP addresses come from?



* In some cases via an NIR such as KRNIC

APNIC Whois Database

What does APNIC do?

Resource service

- IPv4, IPv6, ASNs
- Reverse DNS delegation
- Resource registration
 - Authoritative registration server
 - whois
 - IRR

Policy development

- Facilitating the policy development process
- Implementing policy changes

Information dissemination

- APNIC meetings
- Web and ftp site
- Publications, mailing lists
- Outreach seminars

<http://www.apnic.net/community/lists/>

Training & Outreach

- Training
 - Internet Resource management
 - DNS workshops
- Subsidised for members

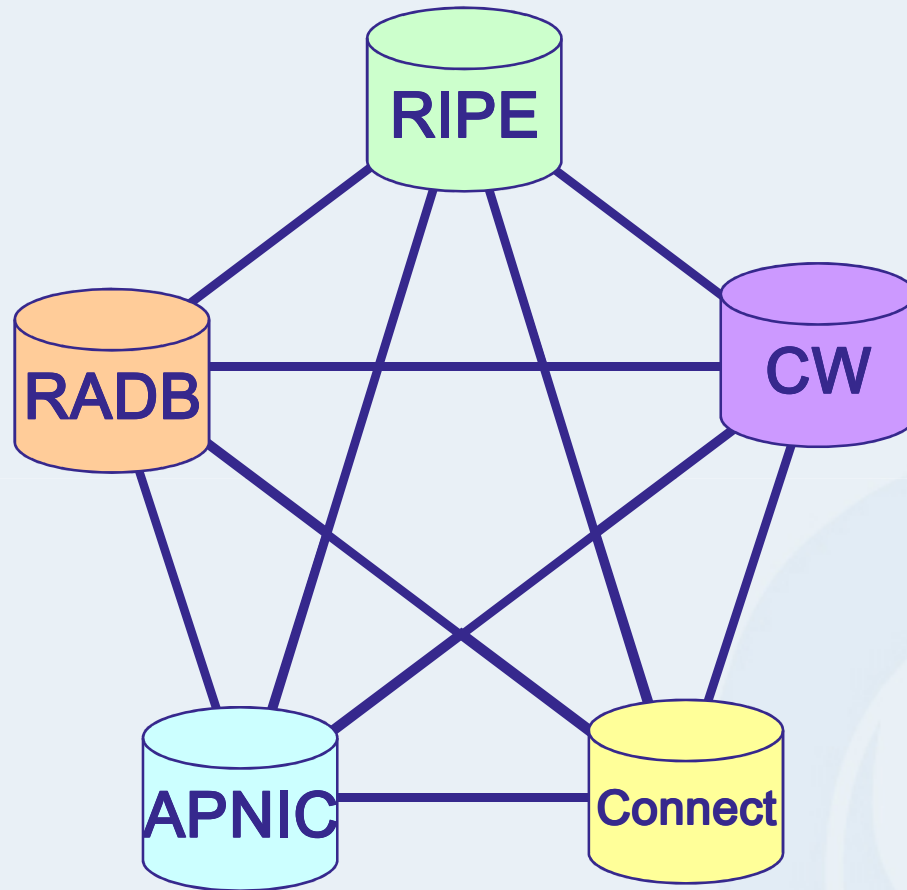
Schedule:

<http://www.apnic.net/training>

What is Whois Database?

- WHOIS is a TCP-based query/response protocol
 - widely used for querying a database in order to determine the custodian of a domain name, an IP address, or an autonomous system number on the Internet.
 - WHOIS lookups were traditionally made using a command line interface
 - Number of simplified web-based tools now exist for looking up
- The WHOIS system originated as a method that system administrators could use to look up information to contact other IP address or domain name administrators
 - almost like a white page

What is Whois Database



- Mirroring is not necessarily bidirectional

- There are various private and public databases
 - ARIN, RIPE, AfriNIC, APNIC, LACNIC, JPNIC, ArcStar, RADB, CW, Optus, Telstra,
- Some of them mirror other databases

Public database

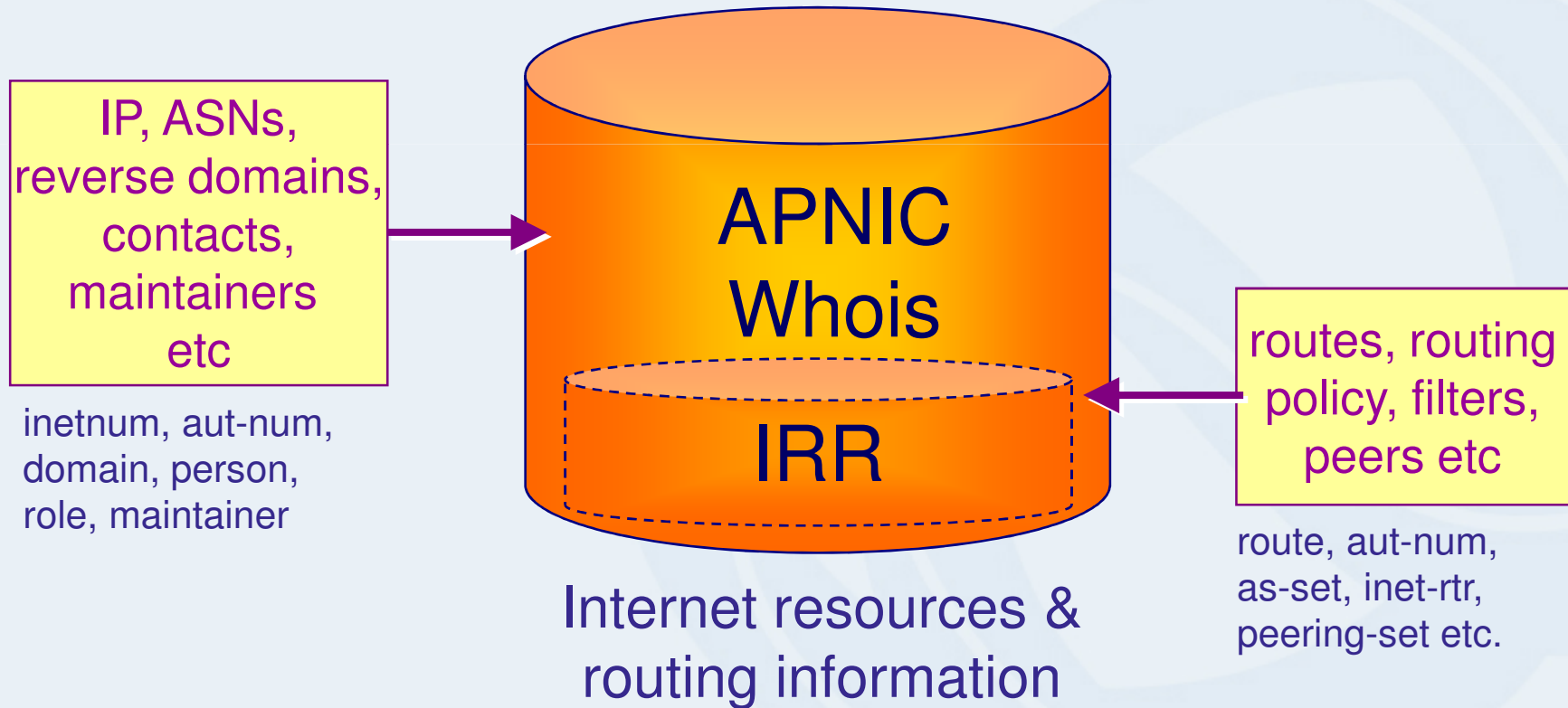
- Public network management database
 - Operated by Internet Registries
 - E.g., APNIC Whois database
 - Public data only
 - Not private data, i.e., customers' assignment data
 - We will discuss this topic later

Tracks network resources

- IP addresses, ASNs, Reverse Domains, Routing policies
- Records administrative information
 - Contact information (persons/roles)
 - Authorisation

APNIC Whois database

- Integrated APNIC Whois Database & Internet Routing Registry



Database object types

OBJECT	PURPOSE
person	Contact person
role	Contact group/roles
inetnum	IPv4 address custodianship
inet6num	IPv6 address custodianship
aut-num	Autonomous System Number
domain	Reverse domain
route	Prefix being announced
mntner	(maintainer) Provide data protection

<http://www.apnic.net/db/>



How to use APNIC Whois database?

Whois database query - clients

- Standard Whois client
 - Included with many Unix distributions
 - RIPE extended Whois client
 - <http://ftp.apnic.net/apnic/dbase/tools/ripe-dbase-client.tar.gz>
- Query via the APNIC website
 - <http://www.apnic.net/apnic-bin/whois2.pl>
- Query clients - MS-Windows etc.
 - Command line query clients, E.g.,
 - <http://gnuwin32.sourceforge.net/packages/jwhois.htm>
 - Web interface
 - Many available (you can easily find them via searching the web)

Why use the whois database?

- Register use of Internet Resources
 - Reverse DNS, IP assignments (public data), etc.
 - Ascertain custodianship of a resource
 - Fulfill responsibilities as resource holder
- Obtain details of technical contacts for a network
 - Investigate security incidents
 - Track source of network abuse or “spam” email

Basic whois database queries

- Unix
 - `whois -h whois.apnic.net <lookup key>`
- Web interface
 - <http://www.apnic.net/apnic-bin/whois2.pl>
- Look-up keys
 - usually the object name
 - Check template for look-up keys



APNIC Whois web query

Welcome to APNIC - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.apnic.net/

Firefox Help Firefox Support Plug-in FAQ Iagu Networks

Home

MyAPNIC

Info & FAQ

Services

Training

Meetings

Membership

Policy

Internet community

Search

Asia Pacific Network Information Centre

Addressing the challenge of responsible Internet resource distribution in the Asia Pacific region

Popular links

- Need IP addresses or an ASN?
- Help tracking spam & hacking
- APNIC Whois Database

About APNIC

- APNIC FAQs
- Reports & statistics
- Contact APNIC
- Employment

Policy

- Mailing list
- Major policies
- How are policies developed?

Research & analysis

- History of the use of Internet resources (BGP, the movie)
- IP addressing in China and the myth of address shortage

Training

- 3-4 September, India

Internet community

- Internet governance
- Partnerships
- Events calendar
- Root DNS nameservers

FAQs | Search | Sitemap

Whois search

- Advanced whois search

News

[26-06-07] [APNIC releases statement on IPv4 consumption](#)

[22-06-07] [IPv6 deployment panel at ICANN meeting](#)

[11-05-07] [APNIC 24 / SANOG 10 fellowship applications now open](#)

NRO news

APNIC is a member of the NRO

[03-05-07] [Afrinic elects Vincent Nguni to Address Council](#)

[02-05-07] [ASO AC selects Raimundo Beca to serve a new term on the ICANN Board](#)

[30-04-07] [ICANN Nominating Committee Extends Deadline for Statements of Interest to 18 May 2007](#)

XML RDF RSS 2.0

Thanks to the [APNIC's sponsors](#): The WIDE Project, Cisco Systems, Telstra, Netapp and Nominum for their support of APNIC.

[Info & FAQ](#) | [Services](#) | [Training](#) | [Meetings](#) | [Membership](#) | [Policy](#) | [Internet community](#) | [Search](#)

Last modified 05:33:27 PM, 09/10/07 | © 1999 - 2007 APNIC Pty. Ltd.
Comments to: webmaster@apnic.net | [Privacy statement](#)

Done

start Microsoft PowerP... Welcome to APNIC - ... EN 5:35 PM

APNIC Whois web query - example

Welcome to APNIC - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.apnic.net/

Firefox Help Firefox Support Plug-in FAQ Iagu Networks

Home

- MyAPNIC
- Info & FAQ
- Services
- Training
- Meetings
- Membership
- Policy
- Internet community
- Search

Asia Pacific Network Information Centre

Addressing the challenge of responsible Internet resource distribution in the Asia Pacific region

Popular links

- Need IP addresses or an ASN?
- Help tracking spam & hacking
- APNIC Whois Database

About APNIC

- APNIC FAQs
- Reports & statistics
- Contact APNIC
- Employment

Policy

- Mailing list
- Major policies
- How are policies developed?

Research & analysis

- History of the use of Internet resources (BGP, the movie)
- IP addressing in China and the myth of address shortage

Training

- 3-4 September, India

Internet community

- Internet governance
- Partnerships
- Events calendar
- Root DNS nameservers

FAQs | Search | Sitemap

Whois search

202.12.29.10 **Go**

- Advanced whois search

News

- [26-06-07] JPNIC releases statement on IPv4 consumption
- [22-06-07] IPv6 deployment panel at ICANN meeting
- [11-05-07] APNIC 24 / SANOG 10 fellowship applications now open

NRO news

APNIC is a member of the NRO

- [03-05-07] AfrinIC elects Vincent Ngundi to Address Council
- [02-05-07] ASO AC selects Raimundo Beca to serve a new term on the ICANN Board
- [30-04-07] ICANN Nominating Committee Extends Deadline for Statements of Interest to 18 May 2007

[XML](#) [RDF](#) [RSS 2.0](#)

Thanks to the [APNIC's sponsors](#): The WIDE Project, Cisco Systems, Telstra, Netapp and Nominum for their support of APNIC.

[Info & FAQ](#) | [Services](#) | [Training](#) | [Meetings](#) | [Membership](#) | [Policy](#) | [Internet community](#) | [Search](#)

Last modified 05:37:20 PM, 09/10/07 | © 1999 - 2007 APNIC Pty. Ltd.
Comments to: webmaster@apnic.net | [Privacy statement](#)

Done DWL: 20.56%

start Microsoft PowerP... Welcome to APNIC - ... EN 5:40 PM

APNIC Whois web query - example



The screenshot shows a Mozilla Firefox browser window with the title "Query the APNIC Whois Database - Mozilla Firefox". The address bar contains the URL "http://wq.apnic.net/apnic-bin/whois.pl". The browser's menu bar includes "File", "Edit", "View", "History", "Bookmarks", "Tools", and "Help". The browser's toolbar shows navigation buttons and a search engine dropdown set to "Google".

The main content area of the browser displays the APNIC website. At the top, there is a navigation menu with links for "Info & FAQ", "Resource services", "Training", "Meetings", "Membership", "Documents", "Whois & Search", and "Internet community". Below the navigation menu, there is a breadcrumb trail: "You're here: Home » Database". A yellow banner reads "Query the APNIC Whois Database".

Under the banner, there is a "Need help?" section with three links: "General search help", "Help tracking spam and hacking", and a note: "To assist you with debugging problems, this whois query was received from IP Address []. Your web client may be behind a web proxy." Below this, there is a copyright notice: "% [whois.apnic.net node-1] % Whois data copyright terms <http://www.apnic.net/db/dbcopyright.html>".

The main query results are displayed in a text-based format:

```
% [whois.apnic.net node-1]
% Whois data copyright terms   http://www.apnic.net/db/dbcopyright.html

inetnum:        202.12.28.0 - 202.12.29.255
netname:        APNIC-AP
descr:          Asia Pacific Network Information Center, Pty. Ltd.
descr:          Level 1 - 33 Park Road.
descr:          Milton QLD 4064
descr:          Australia
country:        AU
admin-c:        AIC1-AP
tech-c:         NO4-AP
mnt-by:         APNIC-HM
changed:        technical@apnic.net 19980918
status:         ASSIGNED PORTABLE
source:         APNIC

role:           APNIC Infrastructure Contact
address:        Level 1
address:        33 Park Road
address:        Milton QLD 4064
country:        AU
phone:          +61 7 3858 3100
fax-no:         +61 7 3858 3199
e-mail:         helpdesk@apnic.net
admin-c:        DNS3-AP
tech-c:         NO4-AP
nic-hdl:        AIC1-AP
remarks:        Infrastructure Contact for APNICs own-use network blocks
notify:         dbmon@apnic.net

```

The browser's status bar at the bottom shows "Done" on the left and "DWL: 20.56%" on the right. The Windows taskbar at the very bottom shows the "start" button, several application icons, and the system tray with the time "5:41 PM".

APNIC Whois command line query - example

```
miwa@durian:~$ whois 202.47.224.0 - 202.47.247.255
% [whois.apnic.net notice]
% Whois data copyright terms http://www.apnic.net/db/dbcopyright.html

inetnum:        202.47.224.0 - 202.47.255.255
netname:        CAT
descr:          Communication Authority of Thailand, CAT
descr:          International Telecommunications Service Provider
country:        TH
admin-c:        TK38-AP
tech-c:         SK79-AP
mnt-by:         APNIC-HM
mnt-lower:      MAINT-TH-THIX-CAT
remarks:        Aggregated block of /18 from smaller blocks.
changed:        hostmaster@apnic.net 20000320
changed:        hm-changed@apnic.net 20030317
status:         ALLOCATED PORTABLE
source:         APNIC

person:         Tanussit Klaimongkol
address:        Data Comm. Dept. (Internet)
address:        CAT Bangkok 10501
address:        Thailand
country:        TH
phone:          +66-2-2374300
fax-no:         +66-2-5063186
e-mail:         ktanus@cat.net.th
nic-hdl:        TK38-AP
mnt-by:         MAINT-TH-THIX-CAT
changed:        ktanus@cat.net.th 20000215
source:         APNIC

person:         Serthsiri Khantawisoote
address:        Data Communication Department, CAT
address:        Bangkok 10501
country:        TH
phone:          +66-2-237-4300
fax-no:         +66-2-506-3186
e-mail:         kserth@cat.net.th
nic-hdl:        SK79-AP
mnt-by:        MAINT-TH-THIX-CAT
changed:        hostmaster@apnic.net 20000320
source:         APNIC
```

Inetnum object

APNIC Whois command line query - example

```
miwa@durian:~$ whois 202.47.224.0 - 202.47.247.255
% [whois.apnic.net node-2]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

inetnum:        202.47.224.0 - 202.47.255.255
netname:        CAT
descr:          Communication Authority of Thailand, CAT
descr:          International Telecommunications Service Provider
country:        TH
admin-c:        TK38-AP
tech-c:         SK79-AP
mnt-by:         APNIC-HM
mnt-lower:      MAINT-TH-THIX-CAT
remarks:        Aggregated block of /18 from smaller blocks.
changed:        hostmaster@apnic.net 20000320
changed:        hm-changed@apnic.net 20030317
status:         ALLOCATED PORTABLE
source:         APNIC

person:         Tanussit Klaimongkol
address:        Data Comm. Dept.(Internet)
address:        CAT Bangkok 10501
address:        Thailand
country:        TH
phone:          +66-2-2374300
fax-no:         +66-2-5063186
e-mail:         ktanus@cat.net.th
nic-hdl:        TK38-AP
mnt-by:         MAINT-TH-THIX-CAT
changed:        ktanus@cat.net.th 20000215
source:         APNIC

person:         Serthsiri Khantawisoote
address:        Data Communication Department, CAT
address:        Bangkok 10501
country:        TH
phone:          +66-2-237-4300
fax-no:         +66-2-506-3186
e-mail:         kserth@cat.net.th
nic-hdl:        SK79-AP
mnt-by:         MAINT-TH-THIX-CAT
changed:        hostmaster@apnic.net 20000320
source:         APNIC
```

202.47.224.0 - 202.47.255.255 = /21

Network name

Network description

Country

nic-handle for administrative and technical contact

Network status

Database source

APNIC Whois command line query - example

```
miwa@durian:~$ whois 202.47.224.0 - 202.47.247.255
% [whois.apnic.net node-2]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

inetnum:        202.47.224.0 - 202.47.255.255
netname:        CAT
descr:          Communication Authority of Thailand, CAT
descr:          International Telecommunications Service Provider
country:        TH
admin-c:        TK38-AP
tech-c:         SK79-AP
mnt-by:         APNIC-HM
mnt-lower:      MAINT-TH-THIX-CAT
remarks:        Aggregated block of /18 from smaller blocks.
changed:        hostmaster@apnic.net 20000320
changed:        hm-changed@apnic.net 20030317
status:         ALLOCATED PORTABLE
source:         APNIC

person:         Tanussit Klaimongkol
address:        Data Comm. Dept. (Internet)
address:        CAT Bangkok 10501
address:        Thailand
country:        TH
phone:          +66-2-2374300
fax-no:         +66-2-5063186
e-mail:         ktanus@cat.net.th
nic-hdl:        TK38-AP
mnt-by:         MAINT-TH-THIX-CAT
changed:        ktanus@cat.net.th 20000215
source:         APNIC

person:         Serthsiri Khantawisoote
address:        Data Communication Department, CAT
address:        Bangkok 10501
country:        TH
phone:          +66-2-237-4300
fax-no:         +66-2-506-3186
e-mail:         kserth@cat.net.th
nic-hdl:        SK79-AP
mnt-by:         MAINT-TH-THIX-CAT
changed:        hostmaster@apnic.net 20000320
source:         APNIC
```

Person object

APNIC Whois command line query - example

```
miwa@durian:~$ whois 202.47.224.0 - 202.47.247.255
% [whois.apnic.net node-2]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

inetnum:        202.47.224.0 - 202.47.255.255
netname:        CAT
descr:          Communication Authority of Thailand, CAT
descr:          International Telecommunications Service Provider
country:        TH
admin-c:        TK38-AP
tech-c:         SK79-AP
mnt-by:         APNIC-HM
mnt-lower:      MAINT-TH-THIX-CAT
remarks:        Aggregated block of /18 from smaller blocks.
changed:        hostmaster@apnic.net 20000320
changed:        hm-changed@apnic.net 20030317
status:         ALLOCATED PORTABLE
source:         APNIC

person:         Tanussit Klaimongkol
address:        Data Comm. Dept. (Internet)
address:        CAT Bangkok 10501
address:        Thailand
country:        TH
phone:          +66-2-2374300
fax-no:         +66-2-5063186
e-mail:         ktanus@cat.net.th
nic-hdl:        TK38-AP
mnt-by:         MAINT-TH-THIX-CAT
changed:        ktanus@cat.net.th 20000215
source:         APNIC

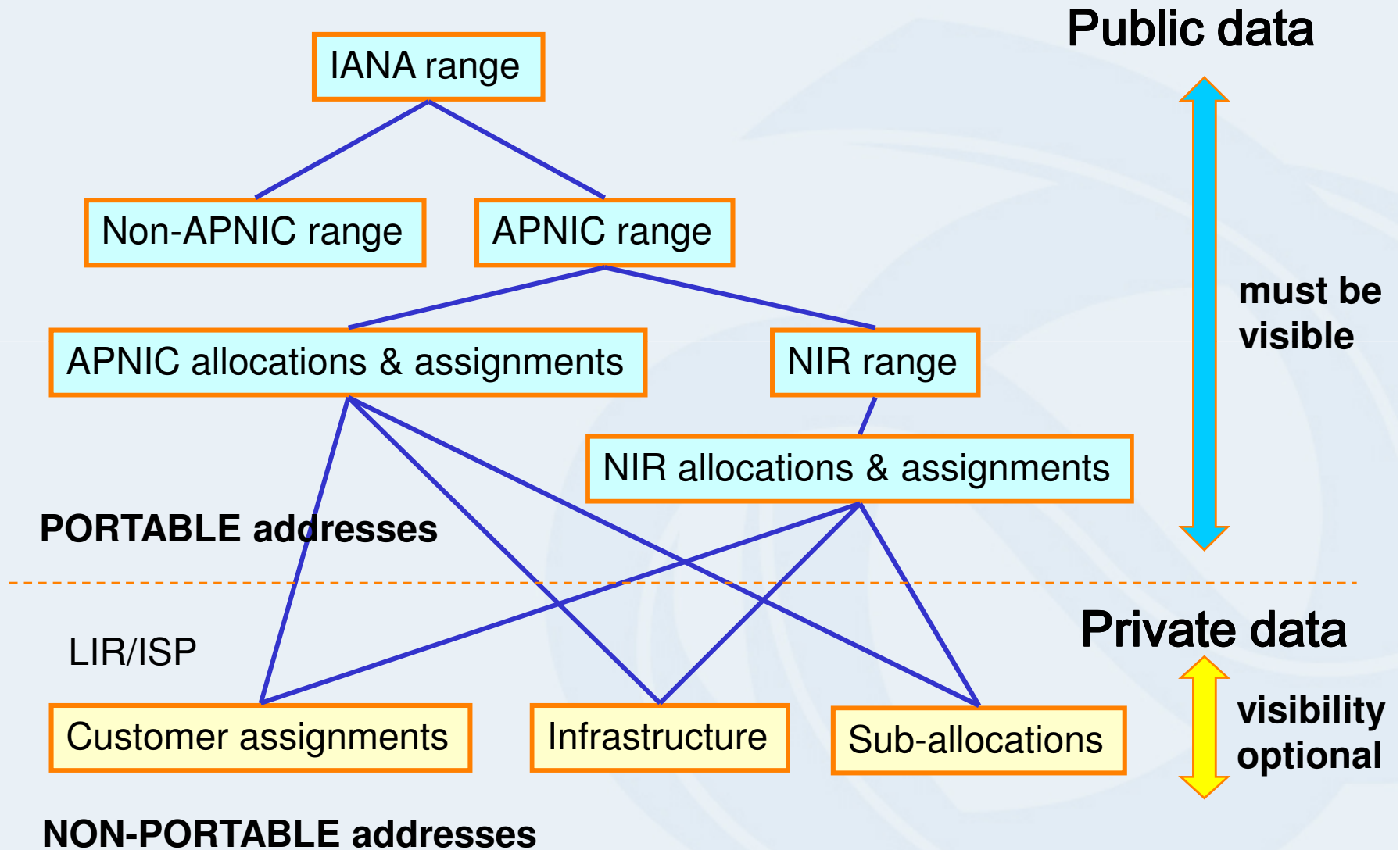
person:         Serthsiri Khantawisoote
address:        Data Communication Department, CAT
address:        Bangkok 10501
country:        TH
phone:          +66-2-237-4300
fax-no:         +66-2-506-3186
e-mail:         kserth@cat.net.th
nic-hdl:        SK79-AP
mnt-by:         MAINT-TH-THIX-CAT
changed:        hostmaster@apnic.net 20000320
source:         APNIC
```

nic-handle for administrative contact

person: Tanussit Klaimongkol
address: Data Comm. Dept. (Internet)
address: CAT Bangkok 10501
address: Thailand
country: TH
phone: +66-2-2374300
fax-no: +66-2-5063186
e-mail: ktanus@cat.net.th
nic-hdl: **TK38-AP**
mnt-by: MAINT-TH-THIX-CAT
changed: ktanus@cat.net.th 20000215
source: APNIC

Referencing to this person object

Public data and private data



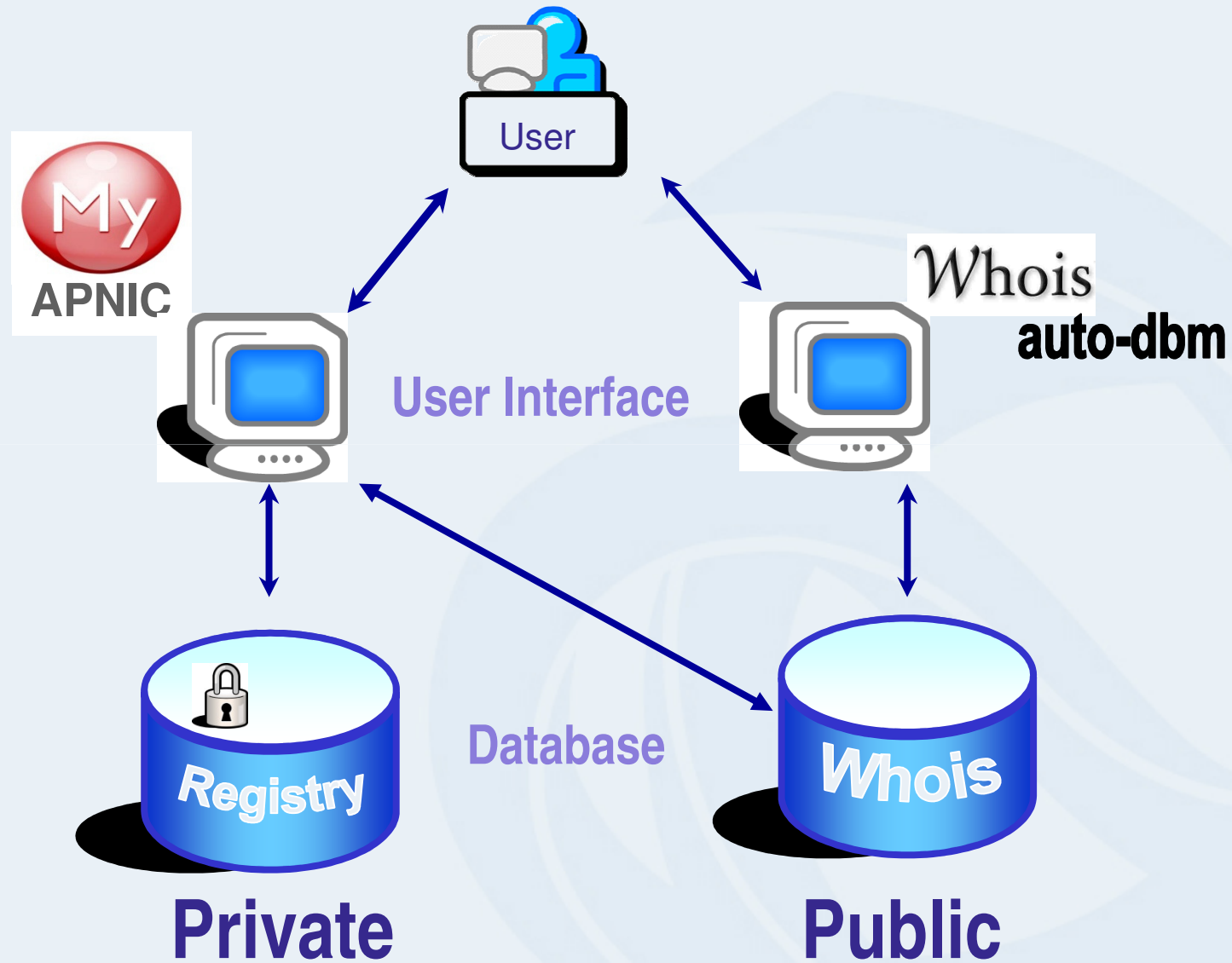
Why private data?

- Customer privacy issues
 - Concerns about publication of customer information
 - Increasing government concern
- APNIC legal risk
 - Legal responsibility for accuracy and advice
 - Damages incurred by maintaining inaccurate personal data
- Customer data is hard to maintain
 - APNIC has no direct control over accuracy of data
 - Freshness of data is up to custodian's update
- Customer assignment registration is still mandatory within APNIC policies

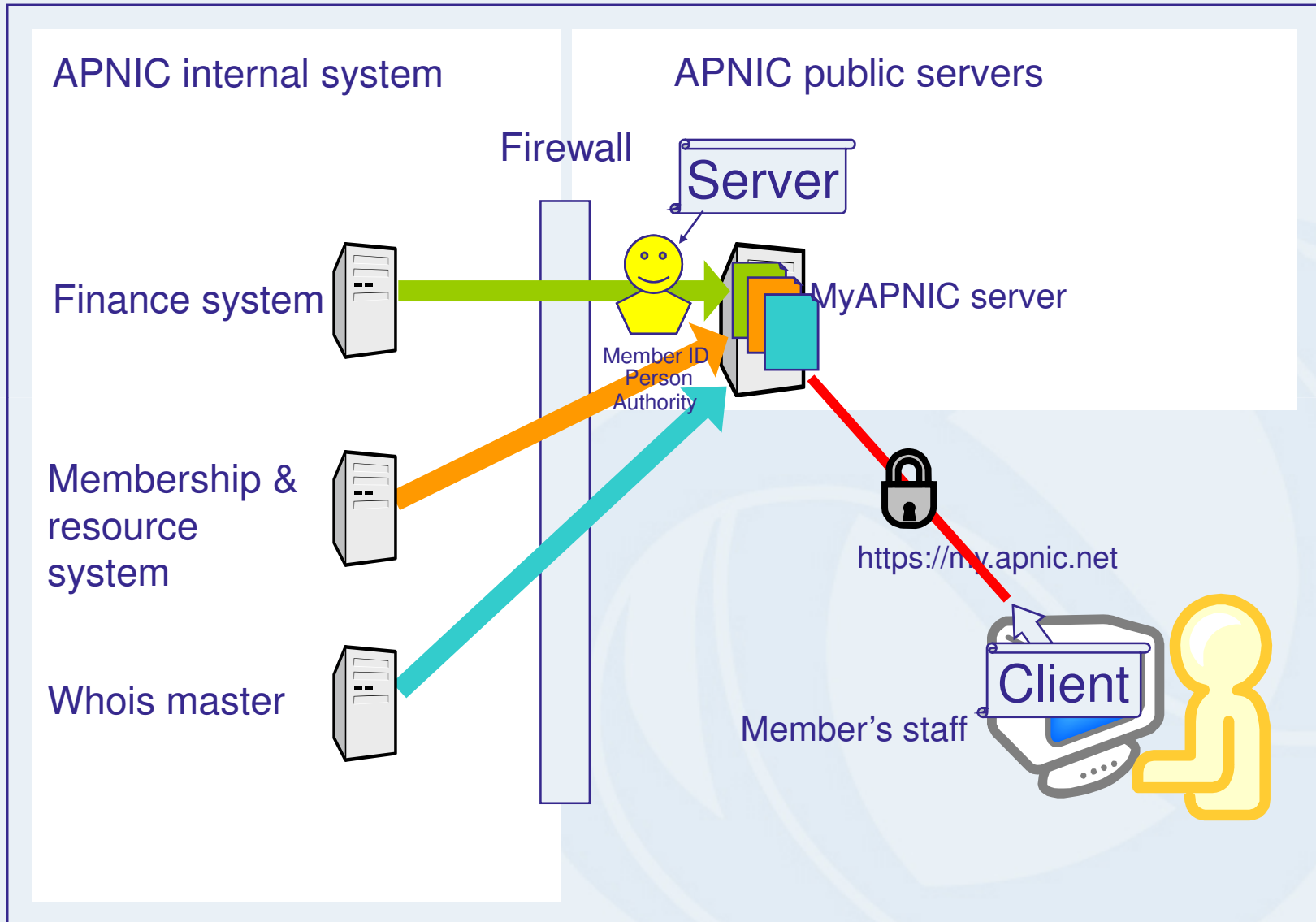
Who can query private data?

- APNIC provides an ISP portal site, MyAPNIC
- APNIC members can query their own account through MyPANIC

Whois database tools



How it works



SANS Internet Storm Centre

Diary Archive

Date	Author	Title
2007-10-12	Jim Clausing	Cyber Security Awareness Tip #12: Managing and Understanding Logs on the Desktop or Laptop (AV, Firewall, or System Logs)
2007-10-11	Mike Poor	Tip of the day: File System Backups
2007-10-10	Lenny Zeltser	Vishing, Skype, and VoIP-Based Fraud
2007-10-10	Lenny Zeltser	Cyber Security Awareness Tip #10: Authentication Mechanisms
2007-10-10	Lenny Zeltser	How to authenticate customers on the phone?
2007-10-09	Swa Frantzen	Adobe mailto vulnerability
2007-10-09	Swa Frantzen	October Black Tuesday overview
2007-10-09	Swa Frantzen	Storm - the paper
2007-10-09	Swa Frantzen	Deobfuscating javascript
2007-10-09	Tom Liston	Follow the Bouncing Malware: Columbus Day

Complete Archive
Search Diaries:

Trends
Top 10 Rising Ports

World Map

© 2000-2007 The SANSSM Institute
SANS Web Privacy Policy: www.sans.org/privacy.php - Web Contact: handlers@sans.org
report bug: [please include debug info \(opens new window\)](#)
Policy On SANS Trademark Usage

Done DWL: 21.03%

start Microsoft PowerPoint ... SANS Internet Storm ... EN 2:56 PM

<http://isc.sans.org/>

All-volunteer effort to detect problems
Data collection, analysis, and warning system

SANS Internet Storm Centre

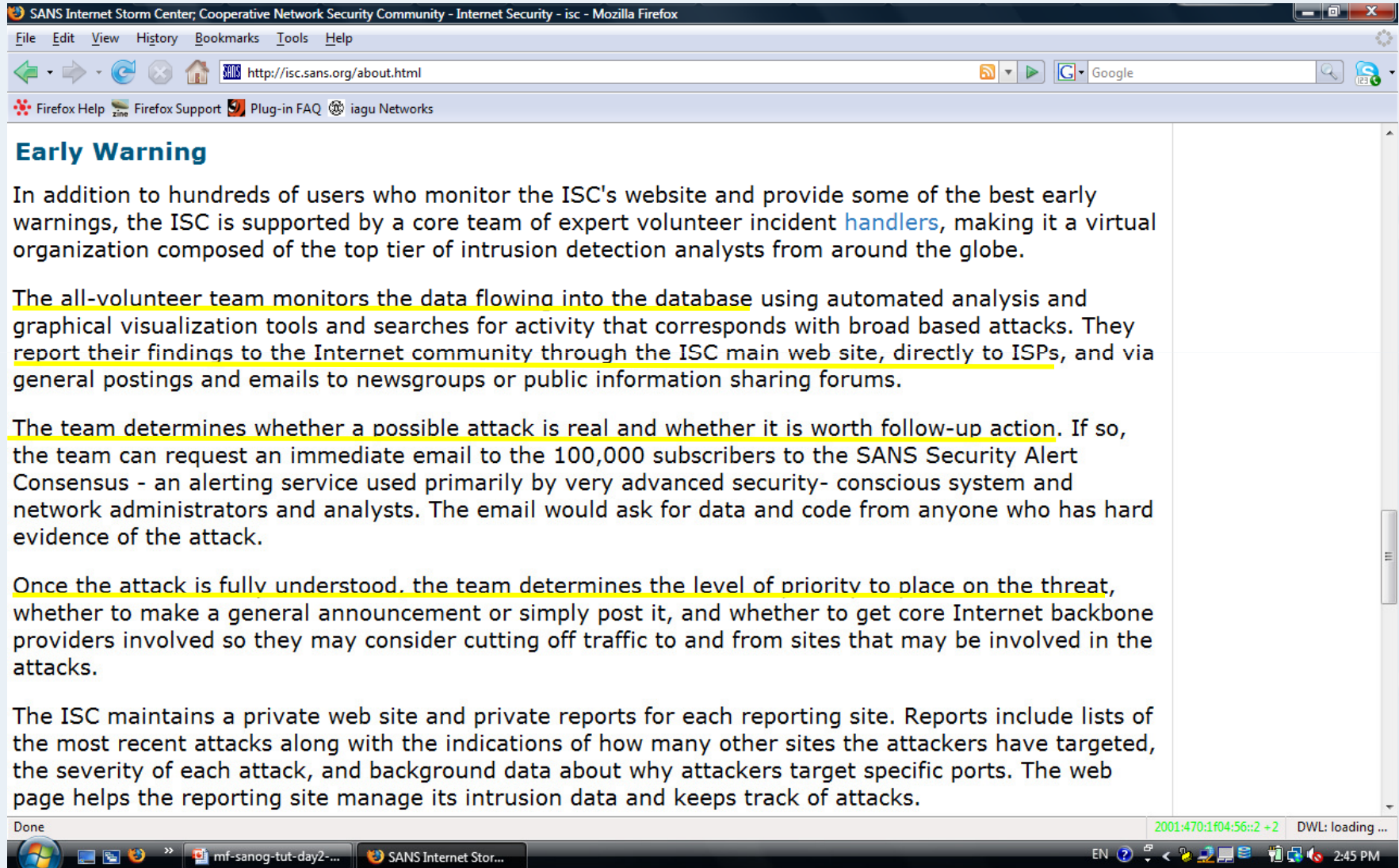
Behind the Internet Storm Center

The ISC relies on an all-volunteer effort to detect problems, analyze the threat, and disseminate both technical as well as procedural information to the general public. Thousands of sensors that work with most firewalls, intrusion detection systems, home broadband devices, and nearly all operating systems are constantly collecting information about unwanted traffic arriving from the Internet. These devices feed the DShield database where human volunteers as well as machines pour through the data looking for abnormal trends and behavior. The resulting analysis is posted to the ISC's main web page where it can be automatically retrieved by simple scripts or can be viewed in near real time by any Internet user.

In many ways, the ISC parallels the data collection, analysis, and warning system used by weather forecasters. For example, the National Weather Service uses small sensors in as many places as possible to report pressure, wind speed, precipitation and other data electronically to regional weather stations. These local stations provide technical support to maintain the sensors, and they summarize and map the sensor data and display it for local meteorologists. They also forward the summarized data to national weather center or transnational weather analysis centers. If analysts are available to monitor the data, they can provide early warnings of storms in their areas. The national and transnational weather analysis centers summarize and map all the regional data to provide an overall picture of the weather. They monitor the data constantly looking for early evidence of major storms and can provide early warnings whenever possible.

Likewise, the Internet Storm Center uses small software tools to send intrusion detection and firewall logs (after removing identifying information) to the DShield distributed intrusion detection system. The ISC's volunteer incident **handlers** monitor the constantly changing database to provide early warnings to the community of major new security threats. The ISC also provides feedback to participating analysis

SANS Internet Storm Centre



The screenshot shows a Mozilla Firefox browser window displaying the SANS Internet Storm Centre website. The address bar shows the URL <http://isc.sans.org/about.html>. The page content includes a section titled "Early Warning" with several paragraphs of text. The browser's status bar at the bottom shows the text "Done" and "2001:470:1f04:56::2 +2 DWL: loading ...".

Early Warning

In addition to hundreds of users who monitor the ISC's website and provide some of the best early warnings, the ISC is supported by a core team of expert volunteer incident **handlers**, making it a virtual organization composed of the top tier of intrusion detection analysts from around the globe.

The all-volunteer team monitors the data flowing into the database using automated analysis and graphical visualization tools and searches for activity that corresponds with broad based attacks. They report their findings to the Internet community through the ISC main web site, directly to ISPs, and via general postings and emails to newsgroups or public information sharing forums.

The team determines whether a possible attack is real and whether it is worth follow-up action. If so, the team can request an immediate email to the 100,000 subscribers to the SANS Security Alert Consensus - an alerting service used primarily by very advanced security-conscious system and network administrators and analysts. The email would ask for data and code from anyone who has hard evidence of the attack.

Once the attack is fully understood, the team determines the level of priority to place on the threat, whether to make a general announcement or simply post it, and whether to get core Internet backbone providers involved so they may consider cutting off traffic to and from sites that may be involved in the attacks.

The ISC maintains a private web site and private reports for each reporting site. Reports include lists of the most recent attacks along with the indications of how many other sites the attackers have targeted, the severity of each attack, and background data about why attackers target specific ports. The web page helps the reporting site manage its intrusion data and keeps track of attacks.

SANS Internet Storm Centre

Participating with the Internet Storm Center

The ISC uses the DShield distributed intrusion detection system for data collection and analysis. DShield collects data about malicious activity from across the Internet. This data is cataloged and summarized and can be used to discover trends in activity, confirm widespread attacks, or assist in preparing better firewall rules.

Currently the system is tailored to process outputs of simple packet filters. As firewall systems that produce easy to parse packet filter logs are now available for most operating systems, this data can be submitted and used without much effort.

DShield is a free service sponsored by the SANS Institute for the benefit of all Internet users. Participants may sign up for DShield at <http://www.dshield.org/signup.html>

You do not *have* to register up in order to submit firewall logs to DShield. You can submit logs anonymously. But there are benefits to registering. Registered users can

- view the firewall logs they submitted to the DShield database (for the last 30 days.)
- get a confirmation of their own submissions emailed to them after every submission.
- optionally enable **Fightback**. DShield will forward selected authenticated submissions to the ISP implicated when we detect that you have been attacked. Registered users can see a summary of Fightback abuse messages that have been sent on their behalf.

SANs Internet Storm Centre

SANS Internet Storm Center; Cooperative Network Security Community - Internet Security - isc - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://isc.sans.org/reports.html

04:50 SANS.org GIAC My ISC port/ip lookup/search: GO

How To Submit Logs

Today's Internet Threat Level: GREEN
Handler on Duty: Joel Esler

Diary Trends Reports About Presentations Top 10
Contact INFOCon Links XML

Handler's Diary: From lolly pops to afterglow; Alex and Mark get the girls; Fake IE 7 update ...

Reports

- Top Ports
- Top Sources
- AS Reports
- Country Reports
- Survival Time
- Trends
- Daily Data Volume (Submissions/day)

Ads by Google

Free Network Monitor Tool
Visibility into IM, VoIP and P2P traffic on
Small Business Security
Try Trend Micro Worry-Free Security Free for
Network Security Scanner
Scan for Open Ports and
Free SANS Top

Transferring data from pagead2.google syndication.com...

mf-sanog-tut-day2-... SANS Internet Stor...

2001:470:1f04:56::2 +2 DWL: loading ...

EN 2:50 PM

SANS Internet Storm Centre

SANS Internet Storm Center; Cooperative Network Security Community - Internet Security - isc - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://isc.sans.org/sources.html

04:52 2008-08-16 16:20:00 SANS.org GIAC My ISC port/ip lookup/search: GO

How To Submit Logs

Today's Internet Threat Level: GREEN

Handler on Duty: Joel Esler

Diary Trends Reports About Presentations Top 10
Contact INFOCon Links XML

Handler's Diary: From lolly pops to afterglow; Alex and Mark get the girls; Fake IE 7 update ...

Top Sources

IP Address	Attacks	Reports	First Seen	Last Seen
202.099.011.099	96,991	1,086,974	2007-11-01	2008-08-11
061.134.056.018	96,878	1,081,472	2008-06-01	2008-08-11
218.075.199.050	95,311	943,899	2008-06-30	2008-08-11
218.064.237.219	93,695	862,013	2008-07-01	2008-08-11
058.020.222.030	89,689	511,539	2008-04-03	2008-08-11
124.165.230.206	83,471	284,849	2008-06-17	2008-08-11
061.132.223.014	76,092	846,828	2008-01-06	2008-08-11
058.241.211.124	71,922	116,527	2008-08-05	2008-08-11
219.153.008.064	67,339	94,157	2008-06-04	2008-08-11
219.134.065.036	63,431	318,026	2008-07-25	2008-08-11
124.227.192.190	62,272	88,577	2008-06-19	2008-08-11
058.042.247.145	60,813	77,778	2008-08-07	2008-08-11

SANS
CYBER DEFENSE INITIATIVE
More Than 20 Courses
Washington DC
December 10-16, 2008

Done 2001:470:1f04:56::2 +2 DWL: loading ...

mf-sanog-tut-day2-... SANS Internet Stor...

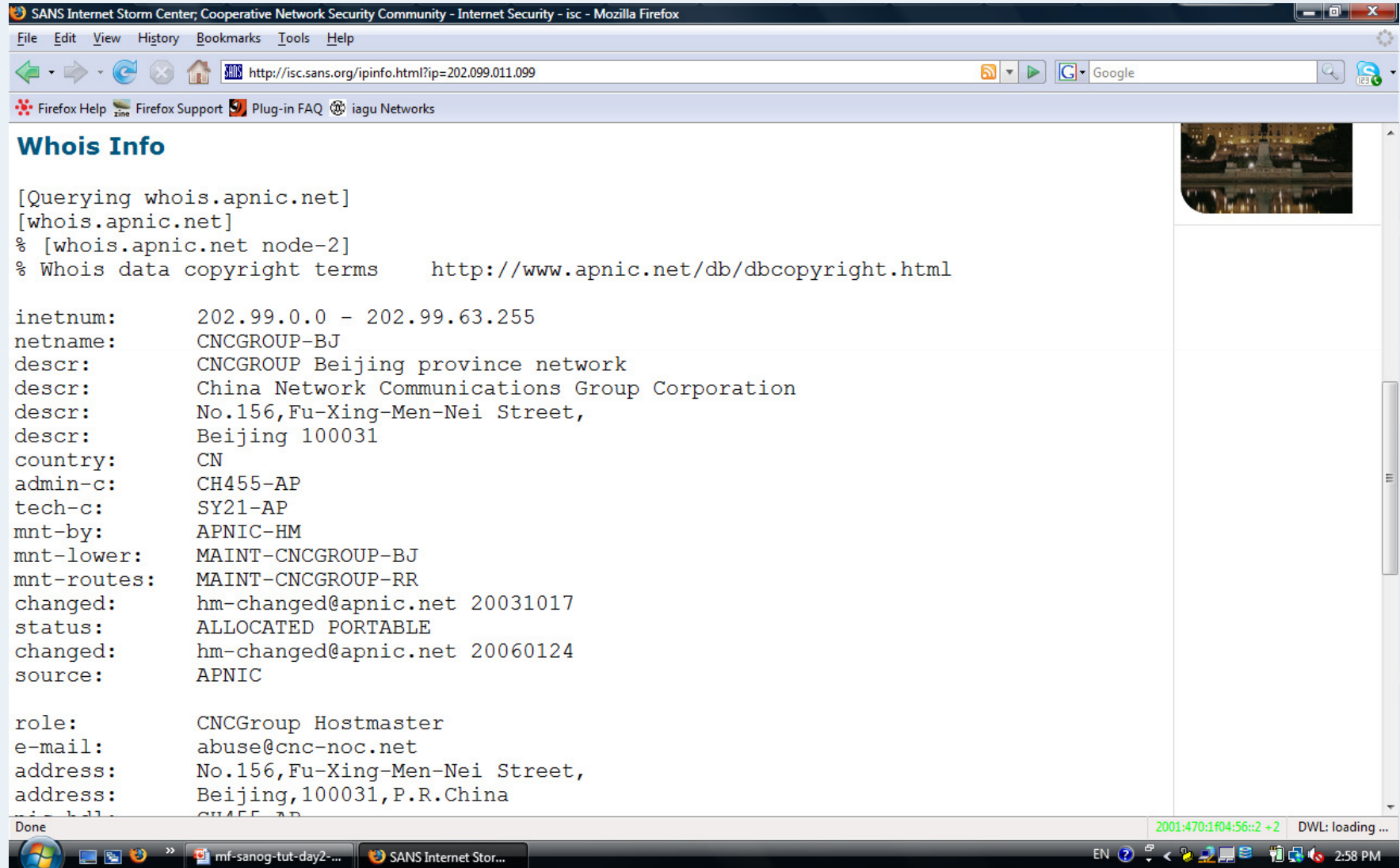
EN 2:53 PM

SANS Internet Storm Centre

The screenshot shows a Mozilla Firefox browser window displaying the SANS Internet Storm Centre website. The address bar shows the URL <http://isc.sans.org/ipinfo.html?ip=202.099.011.099>. The page header includes the SANS logo, navigation links like "GIAC", "My ISC", and "How To Submit Logs", and a search bar. A status bar indicates "Today's Internet Threat Level: GREEN" and "Handler on Duty: Joel Esler". Below this, there are links for "Diary Trends Reports About Presentations Top 10 Contact INFOCon Links XML". A blue link reads "Handler's Diary: From lolly pops to afterglow; Alex and Mark get the girls; Fake IE 7 update ...". The main content area features a section titled "IP Info (202.99.11.99)" with a table of details. To the right of the table is a vertical advertisement for SANS Cyber Defense Initiative, stating "More Than 20 Courses" and "Washington DC December 10-16, 2008". The browser's status bar at the bottom shows "Done", "2001:470:1f04:56::2 +2", "DWL: loading ...", and the time "2:57 PM".

IP Address (click for more detail):	202.99.11.99
Hostname:	202.99.11.99
Country:	CN
AS:	17431
AS Name:	TONET Beijing TONEK Information Technology Development Company
Reports:	1086974
Targets:	96991
First Reported:	2007-11-01
Most Recent Report:	2008-08-11
Comment:	- none -

SANS Internet Storm Centre



SANS Internet Storm Center, Cooperative Network Security Community - Internet Security - isc - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://isc.sans.org/ipinfo.html?ip=202.099.011.099

Firefox Help Firefox Support Plug-in FAQ iagu Networks

Whois Info

[Querying whois.apnic.net]
[whois.apnic.net]
% [whois.apnic.net node-2]
% Whois data copyright terms <http://www.apnic.net/db/dbcopyright.html>

inetnum: 202.99.0.0 - 202.99.63.255
netname: CNCGROUP-BJ
descr: CNCGROUP Beijing province network
descr: China Network Communications Group Corporation
descr: No.156,Fu-Xing-Men-Nei Street,
descr: Beijing 100031
country: CN
admin-c: CH455-AP
tech-c: SY21-AP
mnt-by: APNIC-HM
mnt-lower: MAINT-CNGROUP-BJ
mnt-routes: MAINT-CNGROUP-RR
changed: hm-changed@apnic.net 20031017
status: ALLOCATED PORTABLE
changed: hm-changed@apnic.net 20060124
source: APNIC

role: CNCGroup Hostmaster
e-mail: abuse@cnc-noc.net
address: No.156,Fu-Xing-Men-Nei Street,
address: Beijing,100031,P.R.China

Done 2001:470:1f04:56::2 +2 DWL: loading ...

mf-sanog-tut-day2-... SANS Internet Stor... EN 2:58 PM

So if you are an ISP, what is your responsibility?

- You will be subject to the laws in the places where you operate
- You need to be aware about such laws and keep necessary logs as defined in the law
- So check the legal situation in your own jurisdiction
- Update both public data and private data diligently
 - For your own record keeping purpose too
 - Protect them with the strongest authentication
 - Malicious attack can come from internally too

Network forensics

Acknowledgement

- APNIC conducted extensive researches on the topic of network forensics to develop this module. APNIC appreciate to the following documents provided very useful input:
 - Guide to Integrating Forensic Techniques into Incident Response: Recommendations of the National Institute of Standards and Technology
 - Published by National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce: Available at
 - <http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>
 - Authored by Karen Kent, Suzanne Chevalier, Tim Grance and Hung Dang

Note

- Certain commercial organisations and their products and services may be mentioned in this module. However such identification does not imply recommendation or endorsement by APNIC nor organisations and authors that APNIC referred to develop this module.

Overview

- Digital forensics (forensics) overview
- Forensics process
- Utilised data for forensics process
- Using data from network traffic

Digital forensics overview

- Forensics science
 - The application of science to the law
- Digital forensics (forensics)
 - Also know as
 - Computer and network forensics
 - Application of science to the
 - Identification of data
 - Collection of data
 - Examination of data
 - Analysis of data

Digital forensics overview

- Digital forensics techniques can be used for many purposes
 - Investigation crimes – evidence collection for legal proceedings
 - Internal policy violations – internal disciplinary actions
 - Reconstructing computer security
 - Troubleshooting operational problems – including handling of malware incidents
 - Recovering from accidental system damage
- Without such capability, it will be difficult to determine:
 - What has happened?
 - What damages are incurred
 - Who did cause the problem?
 - How did it happen?
 - How to rectify the problem?
 - How to prevent the future incidents?

Process of digital forensics

- Collection



- Identifying, labelling, recording, and acquiring data from the possible sources while preserving data integrity

- Examination



- Processing collected data forensically, and assessing and extracting data of particular interest while preserving data integrity

- Analysis



- Analysing the results of examination, using legally justifiable methods and techniques

- Reporting

- Reporting the results of the analysis, providing recommendations for improvement of policies, procedures, tools, and other aspects of forensic process

Collection of data

- Identifying possible data sources
 - Typically, desktop computers, servers, network storage devices, and laptops, PDAs, cell phones, digital cameras, digital recorders, audio players and etc.
 - Possible data sources located in other places
 - E.g., Network activity and application usage within an organisation
 - Information may be recorded by other organisations
 - E.g., ISPs

Collection of data

- Analysts should be:
 - mindful of the owner of each data source and the effect on collecting data
 - E.g., getting copies of ISP records typically requires a court order
 - aware of the organisation's policies and legal considerations regarding externally owned property at the organisation's facilities and locations outside the organisation's control
 - E.g., employee's personal laptop, a contractor's laptop
 - E.g., a computer at a telecommuter's home office

Collection of data

- Some useful methods to collect data
 - Keep audit records
 - E.g., Most OSs can be configured to audit and record certain types of events
 - Centralised logging
 - Certain systems and applications forward copies of their logs to secure central log servers
 - Security monitoring controls (E.g., intrusion detection software, anti-virus software, and spyware detection and removal utilities) can generate logs of attacks and intrusions
 - Monitoring of user behaviour
 - Keystroke monitoring
 - Be aware this is a violation of privacy unless users are advised through organisational policy and login banners
 - Employing such method should be discussed with legal advisors and documented clearly in the organisation's policy

Acquiring the data

- Analyst should make a informed decision regarding the prioritisation of data source acquisition
 - Develop a plan to acquire the data
 - Consider likely value, volatility of data and amount of effort required
 - Acquire data
 - Can be acquired through security tools, analysis tools, or other means
 - Can be acquired through forensic tools
 - Verify the integrity of the data
 - Important to prove that the data has not been tampered
 - Can use tools such as message digest

Acquiring the data

- A clear defined chain of custody should be followed to avoid allegations of mishandling or tampering of evidence
 - Keeping a log of every person who had physical custody of the evidence, documenting the actions performed on the evidence and time
 - Storing the evidence in a secure location
 - Making a copy of the evidence and performing examination and analysis using only the copied evidence
 - Verifying the integrity of the original and copied evidence

Data sources

- Using data from data files
- Using data from Operating Systems
- Using data from network traffic
- Using data from applications
- Using data from multiple sources





Data sources

- Network forensics analysis relies on all of the layers
- Hardware layer (=Data link layer) provides information about physical components
- Other layers describe logical aspects
- An analyst can map an IP address (logical identifier at the IP layer) to the MAC address (Media Access Control) of a particular NIC (Network Interface Card = physical identifier at the physical layer)
 - An analyst can identify a host of interest
 - Identifying a host helps to identify most likely being used applications





TCP/IP overview

Application layer	Sends and receives data for particular applications such as Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP)
Transport layer	Provides connection-oriented or connectionless services for transporting application layer services between networks. E.g., Transport Control Protocol (TCP) and User Datagram Protocol (UDP)
Internet Protocol layer (= Network Layer)	Routes packets across networks. IP is the fundamental protocol of this layer. Other protocols are Internet Control Message protocol (ICMP) and Internet Group Management Protocol (IGMP) etc.
Hardware layer (=Data Link Layer)	Handles communications on the physical network components. Well known data link layer protocol is Ethernet.

TCP/IP overview

<p>Application layer</p> 	<p>Sends and receives data for particular applications such as Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP)</p>
<p>Transport layer</p> 	<p>Provides connection-oriented or connectionless services for transporting application layer services between networks. E.g., Transport Control Protocol (TCP) and User Datagram Protocol (UDP)</p>
<p>Internet Protocol layer (= Network Layer)</p> 	<p>Routes packets across networks. IP is the fundamental protocol of this layer. Other protocols are Internet Control Message protocol (ICMP) and Internet Group Management Protocol (IGMP) etc.</p>
<p>Hardware layer (=Data Link Layer)</p> 	<p>Handles communications on the physical network components. Well known data link layer protocol is Ethernet.</p>

TCP/IP overview

Application layer  ↑	Sends and receives data for particular applications such as Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP)
Transport layer  ↑	Provides connection-oriented or connectionless services for transporting application layer services between networks. E.g., Transport Control Protocol (TCP) and User Datagram Protocol (UDP)
Internet Protocol layer (= Network Layer)  ↑	Routes packets across networks. IP is the fundamental protocol of this layer. Other protocols are Internet Control Message protocol (ICMP) and Internet Group Management Protocol (IGMP) etc.
Hardware layer (=Data Link Layer)  ↑	Handles communications on the physical network components. Well known data link layer protocol is Ethernet.

IPv4 datagram header

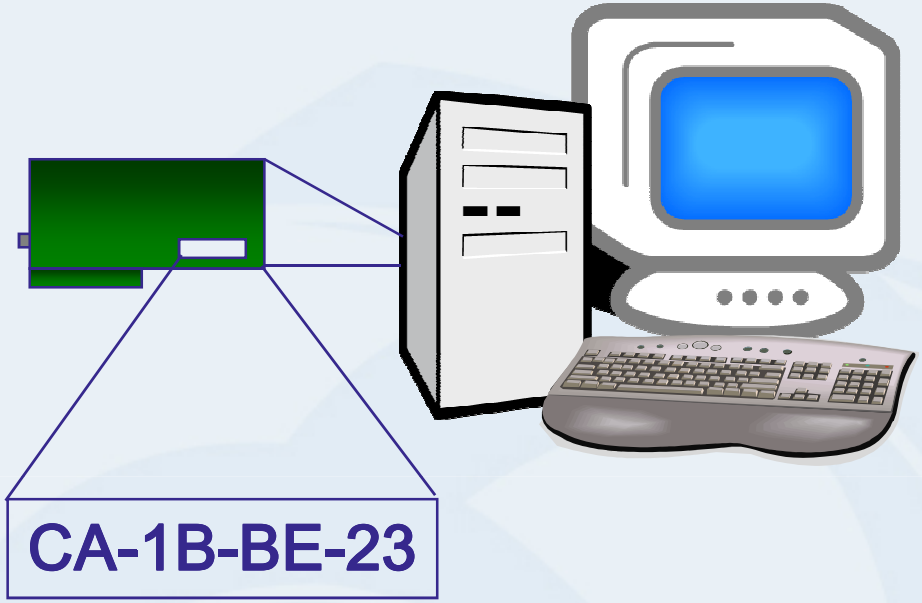
VER 4 bits	HLEN 4 bits	DS (TOS) 8 bits	Total length 16 bits	
Identification 16 bits		Flag S 3 bits	Fragmentation offset 13 bits	
Time to live 8 bits	Protocol 8 bits	Header checksum 16 bits		
Source IP address				
Destination IP address				
Options				

Data sources

Email header

Source IP address
202.12.29.203

C:\arp -a 202.12.29.203			
Internet address	Physical address	Type	
202.12.29.203	CA-1B-BE-23	dynamic	



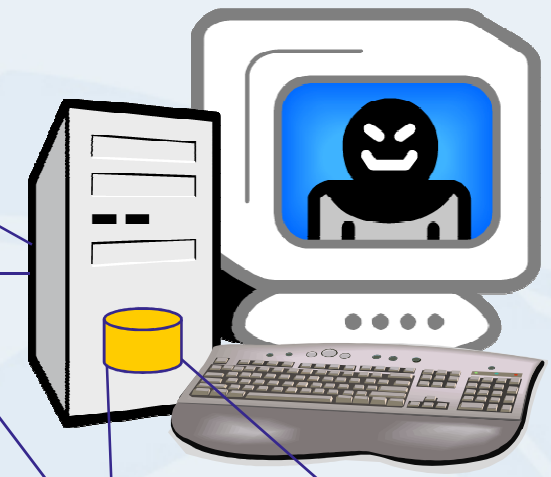
Data sources

Email header

Source IP address
202.12.29.203

C:\arp -a 202.12.29.203			
Internet address	Physical address	Type	
202.12.29.203	CA-1B-BE-23	dynamic	

CA-1B-BE-23



Hard disc content

- Installed applications
- Data

Network traffic data source

- Typically several types of information sources are available
 - Firewalls and routers
 - Packet sniffers
 - Protocol analysers
 - Intrusion Detection Systems (IDSs)
 - Security event management tools
 - Network forensic analysis tools

Firewalls and routers

- Firewall and routers examine network traffic and permit or deny it based on a set of rules
- They can be configured to log traffic information. E.g.,
 - Date and time the packet was processed
 - The source and destination IP addresses
 - The transport layer protocol (e.g., TCP, UDP)
 - Basic protocol information (e.g., TCP or UDP port numbers, ICMP type and code)

Packet sniffers and protocol analysers

- Packet sniffers are designed to monitor network traffic by capturing packets
 - Typically used to capture a particular type of traffic for troubleshooting or investigative purposes
 - Place the NIC in promiscuous mode
 - NIC accepts all incoming packets that it sees, regardless of their intended destinations
 - An analysis can configure the sniffer with particular criteria (E.g., certain TCP ports, certain source or destination IP addresses)
- Most of packet sniffers are also protocol analysers
 - They can reassemble streams from individual packets and decode communications

Intrusion Detection Systems

- Network IDSs perform:
 - packet sniffing to identify suspicious activity
 - analyse network traffic to identify suspicious activity
 - record relevant information
- Typically records:
 - Traffic information: e.g., date and time, source and destination IP addresses, protocol, protocol related information
 - Application specific information: e.g., username, filename, command, status code
 - Other information: possible intent of the activity

Remote access

- Remote access servers:
 - Devices such as VPN (Virtual Private Network) gateways and modem servers that facilitate connections between networks
 - Typically record
 - the origin of each connection and
 - might also indicate user account authentication information for each session
 - If remote access server assigns an IP address to a remote user such information can be logged too
- Applications designed to provide remote accesses
 - E.g., SSH (Secure Shell), Telnet, terminal servers, and remote control software
 - Such applications can be configured to log basic information for each connections (e.g., source IP addresses and user accounts)

Security Event Management Software

- Security Event Management (SEM) software:
 - Can increase accessibility of many sources of network traffic information through a single interface
 - Importing security event information from various network traffic-related security event data sources (e.g., IDS logs, firewall logs)
 - Correlating events among the sources
 - Identifying related events by matching IP addresses, timestamps, and other aspects

Network Forensic Analysis Tools

- Network Forensic Analysis Tools (NFAT):
 - Typically provide a combined functionalities of packet sniffers, protocol analysers, and SEM software in a single product
 - Their focuses are typically on collecting, examining, and analysing network traffic

Other sources

- Dynamic Host Configuration Protocol Servers (DHCP)
 - They may contain assignment logs including the MAC address, the IP address assigned to that MAC address, and the assignment time
- Network Monitoring Software
 - To observe network traffic and gather statistics
 - E.g., the amount of bandwidth typically consumed by various protocols, payload size and the source and destination IP addresses and ports for each packets
- Client/Server applications
- Hosts' network configuration and connections
- **Internet Service Provider (ISP) records**
 - ISP may collect network traffic-related data as part of their normal operations
 - Usual ISP records often might be kept for days or hours based on their business procedures

Legal considerations

- Collecting network traffic has legal implications
 - Information with privacy or security implications
 - Passwords the contents of emails, users' access records etc.
 - Organisations should have policies in regards with the monitoring networks, handling collected information and data retention policy
 - E.g., warning banners to systems that indicate network monitoring
 - Data collection after certain incidents
 - Important to follow consistent processes and to document all actions performed
 - E.g., Data collections on a particular user should be initiated only after the successful completion of a formal request and approval process
 - Organisations should have policies
 - What types of monitoring can and can not be performed without approval
 - Procedures of the request and approval process
 - Preserve original logs

Legal considerations - ISPs

- Large number of ISPs may require a court order before providing any information related to suspicious network activities
 - Suspicious packets passed through their infrastructure
 - This helps to preserve privacy and reduces the burden on and liability of the ISPs
 - It also slows down investigative process
 - Traffic of an ongoing network-based attack can go through several ISPs
 - It is hard to trace its source



Preservation vs. retention

- ISP typically discard any log file that's no longer required for business reasons
 - Network monitoring, fraud prevention or billing disputes
- US law enforcement groups claim by the time they contact ISPs, customers records may have been deleted in the routine course of business
 - Industry representatives say that if police respond to incidents promptly it's difficult to imagine any investigations to be imperilled
- Unclear which data retention law is required

Ref: cnet news.com "FBI director wants ISPs to track users, by D. McCullagh

http://news.com.com/FBI+director+wants+ISPs+to+track+users/2100-7348_3-6126877.html, accessed on 07/09/2007

Does police contact APNIC?

Does police contact APNIC?

- Sometimes polices contact APNIC as a part of their computer crime investigation
- Sometimes polices visit the APNIC's office from various parts of the world to investigate details of a specific network

What information can APNIC provide?

- Public data in the APNIC Whois DB is publicly available
 - Anyone knowing how to query can conduct network search
 - The police have as much right to search it as anyone else
 - APNIC can provide some advice to the police
 - How the Whois DB works?
 - What the various fields mean?
 - How best to search it?

But remember...

- Information accuracy and freshness is up to organisations which are custodians of each address block
- Most likely no customer assignment details can be found on the public database
 - Only the ISP who assign the IP address to their customers can see details

Information on direct allocation and assignment made by APNIC

- If a custodian of an address block directly allocated or assigned by APNIC is investigated
 - APNIC may be asked to provide more detailed information than the public Whois DB such as billing details or other contact information
 - In such case, generally a court order or warrant will be required as APNIC has non-disclosure agreement with its members
 - Remember, APNIC only knows about the address registered in the Whois DB.
 - APNIC has no information about who is actually using the address

Specific network traffic information

- APNIC does not have any information about network traffic information
 - Who used which IP address at what time
 - Such information, usually only available through logs held by the ISP, if they have not deleted them yet
- If the police is looking for such information, APNIC suggests them to contact the ISP

Thank you!