AFRINIC
The Internet Numbers Registry for Africa

# How AFRINIC can support Law Enforcement in Cybercrime Investigation

Alan Barrett, AFRINIC CEO

African Forum on Cybercrime

Addis Ababa, Ethiopia, 16-18 October 2018

# About AFRINIC

- AFRINIC is the Regional Internet Registry for Africa, including nearby islands
- Responsible for issuing Internet number resources (IP addresses and ASNs) throughout the continent
  - >1600 members from all over Africa
  - Most members are ISPs
  - Some are universities, governments, commercial enterprises
- AFRINIC keeps records of which IP addresses are allocated or assigned to each member
- These records may be useful to investigators

# The WHOIS database

- AFRINIC keeps a database of all number resources issued to our members
  - Called the “WHOIS” database
  - Accessed via a standard protocol, or a web form
- Includes every block of IP addresses issued by AFRINIC
- Other Regional Internet Registries (RIRs) do the same in other parts of the world

# What’s included

- Included:
  - Block of IP addresses allocated by AFRINIC
  - Organisation name (AFRINIC member)
  - Contact people (admin contact, tech contact)
  - Address, phone number, email address
- Sometimes included:
  - Smaller blocks given by ISPs to their customers (business customers, or smaller ISPs)
- Not included:
  - IP addresses for individual users

# Access policy

- The WHOIS database is publicly accessible
  - Some items of information may be hidden
- Web interface at http://whois.afrinic.net
- Command line interface available in some operating systems (e.g. Unix/Linux)
- Use for legitimate investigation or operational purposes, not for spam, market research, etc.
- Bulk access can be arranged
- AFRINIC may also have non-public information, which is unlikely to help investigators, but could potentially be requested via court order.

# Investigation steps

- Suppose that the early part of an investigation gives you an IP address implicated in cybercrime
- Look up the IP address in AFRINIC (or other RIR) WHOIS database
- WHOIS lookup provides an organisation name (typically an ISP), country, contact person names, address, phone number
- Approach the ISP for more information about the individual who used that IP address at that time

# Example Query

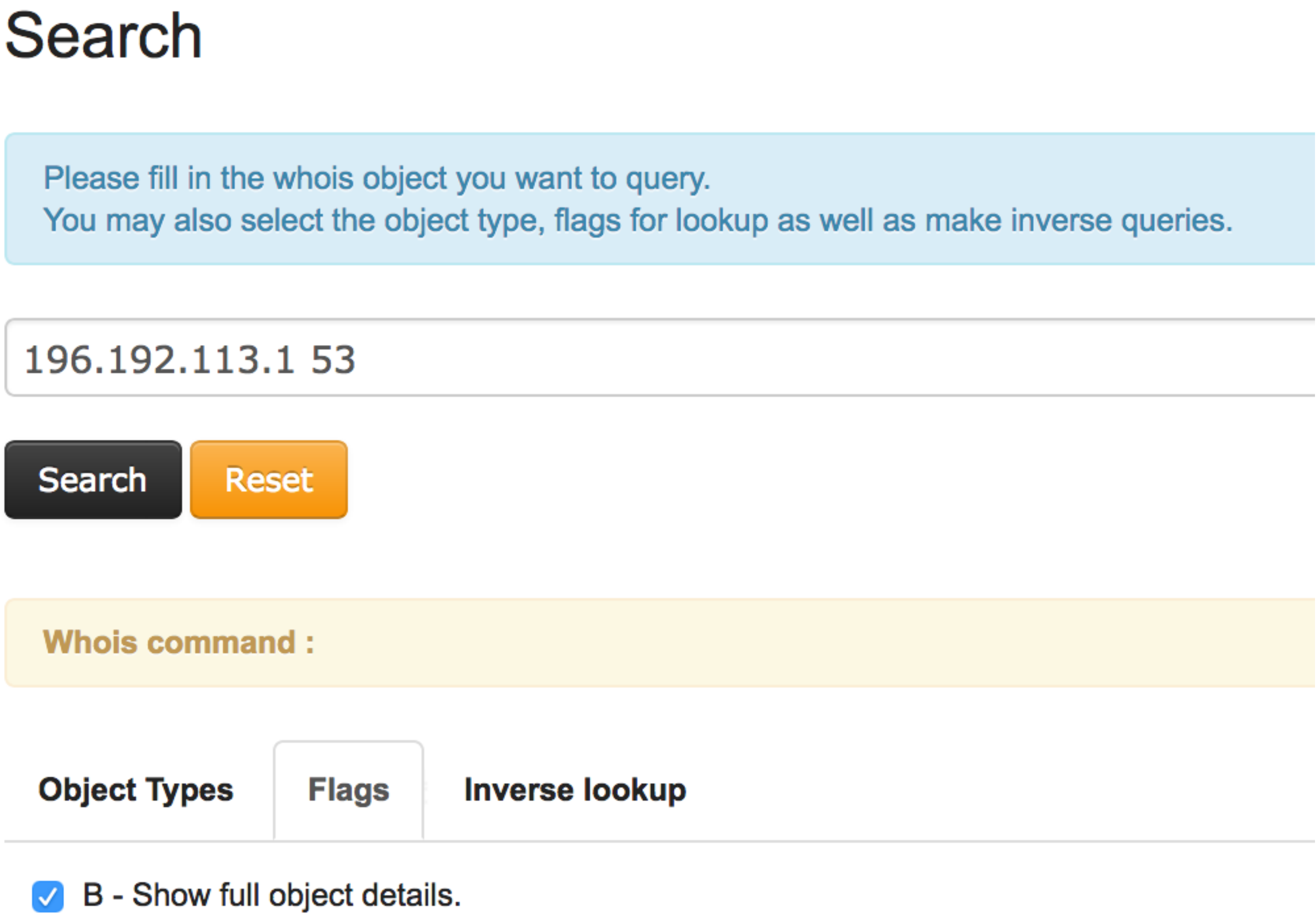
- Example: Looking up an IP address

- Go to the web form at whois.afrinic.net

- Enter the IP address
- Also select the “B” flag, or else email addresses will be hidden
- Click the SEARCH button

# Example Query

https://whois.afrinic.net/



## Search

Please fill in the whois object you want to query.
You may also select the object type, flags for lookup as well as make inverse queries.

```
196.192.113.1 53
```

**Whois command :**

☑ B - Show full object details.

# Example Result

- Result is several paragraphs of information.
  - First paragraph is most relevant. “inetnum” is a block of IP addresses, containing the address you asked about

```
inetnum:        196.192.112.0 - 196.192.113.255
netname:        AFRINIC-MU-OPS
descr:          AfriNIC Ltd
country:        MU
org:            ORG-AFNC1-AFRINIC
admin-c:        CA15-AFRINIC
tech-c:         IT7-AFRINIC
mnt-by:         AFRINIC-HM-MNT
mnt-lower:      AFRINIC-IT-MNT
mnt-routes:     AFRINIC-IT-MNT
mnt-irt:        IRT-AFRINIC-IT
changed:        hostmaster@afrinic.net 20151027
source:         AFRINIC
parent:         196.0.0.0 - 196.255.255.255
```

Yellow: database key; green: information; blue: reference to related informaiton

Inetnum: The block of IP addresses.
Descr: free text description, sometimes misleading.
Country: 2-letter code.
Org: Organisation handle.
Tech-c, admin-c: Technical contact, admin contact.
Mnt-by: Who may edit this record.
Mnt-irt: refers to an abuse contact.
Parent: Larger block of IP addresses that contains this block.

Org, admin-c, tech-c, mnt-* are “handles” to be used in a subsequent database lookup.

# The “org” is the organisation

```
organisation:   ORG-AFNC1-AFRINIC
org-name:       African Network Information Center - ( AfriNIC Ltd. )
org-type:       RIR
country:        MU
address:        11th Floor, Standard Chartered Tower
address:        19, Cybercity
address:        Ebène
phone:          tel:+230-403-5100
fax-no:         tel:+230-466-6758
e-mail:         contact@afrinic.net
admin-c:        CA15-AFRINIC
tech-c:         IT7-AFRINIC
mnt-ref:        AFRINIC-HM-MNT
mnt-ref:        AFRINIC-IT-MNT
mnt-ref:        AFRINIC-DB-MNT
notify:         hostmaster@afrinic.net
mnt-by:         AFRINIC-HM-MNT
changed:        hostmaster@afrinic.net 20180906
source:         AFRINIC
```

Organisation: The ”handle” for this organisation. You saw it before as “org” under the address block.

Org-name, address, phone, fax-no: Self-explanatory.
Admin-c, tech-c: Admin contact and tech contact for the organisation.

Admin-c and tech-c handles can be used in a subsequent database lookup.

Yellow: database key; green: information;
blue: reference to related informaiton

# The “tech-c” and “admin-c” are responsible people

```
person:       CTO AFRINIC
address:       11th Floor, Standard Chartered Tower
address:       Cybercity, Ebène
address:       Mauritius
phone:        tel:+230-403-5100
e-mail:       cto@afrinic.net
nic-hdl:      CA15-AFRINIC
mnt-by:       CTO-MNT
changed:        daniel@afrinic.net 20171108
source:       AFRINIC

person:       Infrastructure Team
address:       AFRINIC Ltd
address:       11th Floor, Standard Chartered Tower
address:       Cybercity, Ebène
address:       Mauritius
phone:        tel:+230-403-5100
e-mail:       sysadmin@afrinic.net
nic-hdl:      IT7-AFRINIC
mnt-by:       AFRINIC-IT-MNT
changed:        daniel@afrinic.net 20171108
source:       AFRINIC
```

Yellow: database key; green: information; blue: reference to related informaiton

Nic-hdl: The “handle” for this person, which you have seen before under “tech-c” and “admin-c” on previous slides.

Person: Sometimes a person’s name, or sometimes a job function.
Address, phone, e-mail: self-explanatory.

Email address is hidden if you do not select the -B option on the web form.

# Sometimes there is also a “route” object, which may help expand the search to another ISP

```
route:          196.192.113.0/24
descr:           AFRINIC-MUR-OPS
origin:         AS37708
mnt-by:           AFRINIC-IT-MNT
changed:            madhvi@afrinic.net 20151030
source:           AFRINIC
```

Route: Another way of referring to a block of IP addresses, which contains the address of interest.
Descr: free text description, sometimes misleading.
Origin: An “autonomous system number” identifying an ISP.

You can use the AS number in a subsequent WHOIS lookup, which might lead you to a different ISP. (The ISP that routes the traffic is not always the same as the ISP that manages the addresses.)

Yellow: database key; green: information; blue: reference to related informaiton

# Follow pointers to related information

- Lookup by IP address (IPv4 or IPv6) or ASN
- Result gives “handles” for organisation, admin contact, tech contact, etc.

- Then perform another lookup by handle
- Result gives name, email address, phone number, etc.

- The second lookup by handle might be done for you automatically

# What you get from WHOIS

- You usually get an ISP name, address, and contact details.
- It could also be an organisation other than an ISP.
- You sometimes get an anonymised reference to a customer of an ISP.
- Information applies to a block of many IP addresses.

## What you do not get

- WHOIS will not provide information about individual IP addresses, or the people using them.
    - The information in WHOIS is for blocks of IP addresses.
- You can approach the ISP for more information about the individual IP address, and the person using it at a specific time.

# WHOIS Data Accuracy

- AFRINIC members are contractually obligated to keep their contact information up to date
  - and to register similar information for their large customers
- We understand that LEAs are concerned about accuracy
- AFRINIC is proactively contacting all our members to check the accuracy of the contact information
  - As of Q3 2018, we have contacted 100% of members, and >80% have verified their information

# More help

- Article on tracing the culprits:
- http://www.afrinic.net/en/library/corporate-documents/769-spam-hacking-and-network-abuse-tracing-the-culprits

- Ask us for help: contact@afrinic.net
- We will assist you in interpreting public WHOIS results, suggesting where to look next
- We can’t release non-public information, unless you have a court order valid in Mauritius
  - Don’t worry, the public information is usually enough to identify the correct ISP.

# Other things AFRINIC does

- AFRINIC holds two public meetings per year
  - See http://meeting.afrinic.net
  - Technical presentations
  - Discussion of policy
- AFRINIC Government Working Group (AfGWG)
  - Aims to strengthen relationships with regulators and law enforcement
  - Closed side-meeting during the larger AFRINIC meetings
  - Mailing list
- Planning to develop training specifically to help LEAs interact with AFRINIC

# Policy Development Opportunity

- AFRINIC policies define the rules for how Internet number resources are managed
- Policies are set by the community through discussion, ratified by the Board
- Discussion is open to anybody with an interest

- LEAs can get involved in policy discussion
- In some other regions, LEAs have started discussions on policy changes to address WHOIS data accuracy, and contact points for dealing with network abuse

# Talk to us

- AFRINIC would like to learn more about the challenges faced by law enforcement
- How we can help, while respecting our members' privacy?
- You are welcome to participate in AFRINIC public policy process, attend AfGWG meetings, subscribe to AfGWG mailing list.

# Thank you for your Attention

# Questions?

twitter.com/ afrinic

afrinic

flickr.com/

afrinic

facebook.com/

afrinic

linkedin.com/company/

afrinic

youtube.com/

afrinic

www.

media

.net