

RIPE 90, Lisbon  
12-16 May 2025



# Who Actually Is? Finding the Companies Behind the Networks



Joshua Levett, Dr Vassilios Vassilakis, Dr Poonam Yadav



Engineering and  
Physical Sciences  
Research Council



# WHOIS

139.162.230.184

```
inetnum:        139.162.0.0 -
                  139.162.255.255
netname:        EU-LINODE-20141229
descr:          139.162.0.0/16
org:            ORG-LL72-RIPE
country:        US
admin-c:        DUMY-RIPE
abuse-c:        LAS85-RIPE
tech-c:         DUMY-RIPE
status:         LEGACY
remarks:        Please send abuse
                  reports to abuse@linode.com
mnt-by:         linode-mnt
created:        2004-02-02T16:20:09Z
last-modified:  2022-12-12T21:26:29Z
source:        RIPE
```

# WHOIS...?

ORG-LL72-RIPE

```
organisation:  ORG-LL72-RIPE
org-name:      Linode, LLC
country:       US
org-type:      LIR
address:       Dummy address for
                ORG-LL72-RIPE
e-mail:        unread@ripe.net
abuse-c:       LAS85-RIPE
mnt-ref:       RIPE-NCC-HM-MNT
mnt-ref:       linode-mnt
mnt-by:        RIPE-NCC-HM-MNT
mnt-by:        linode-mnt
created:       2009-11-02T13:42:45Z
last-modified: 2020-12-16T13:00:31Z
source:        RIPE
```

# WHOIS...?

ORG-LL72-RIPE

```
organisation:  ORG-LL72-RIPE
org-name:      Linode, LLC
country:       US
org-type:      LIR
address:
```

**AH, SO IT MUST BE LINODE, LLC**

```
Dummy address for
ORG-LL72-RIPE
e-mail:        admin@linode.com
abuse-mailbox: abuse@linode.com
mnt-ref:       RIPE-NCC-HM-MNT
mnt-ref:       linode-mnt
mnt-by:        RIPE-NCC-HM-MNT
mnt-by:        linode-mnt
created:       2009-11-02T13:42:45Z
last-modified: 2020-12-16T13:00:31Z
source:        RIPE
```

```
> traceroute
139.162.230.184
```

```
 1    2 ms    1 ms    1 ms    192.168.1.1
 2    *      *      *      Request timed out.

10    *      *      *      Request timed out.
11   26 ms   24 ms   31 ms   ae6.....akamai.com [23.197.64.72]
12   30 ms   29 ms   23 ms   ae1.....akamai.com [23.197.64.69]
13   51 ms   22 ms   22 ms   ae23.....akamai.com [23.210.48.109]
14   24 ms   21 ms   25 ms   10.207.32.2
15   37 ms   25 ms   21 ms   10.207.35.19
16   24 ms   27 ms   18 ms   10.207.6.131
17   28 ms   22 ms   29 ms   ns2.krystal.uk [139.162.230.184]
```

```
> traceroute  
139.162.230.184
```

```
1      2 ms      1 ms      1 ms      192.168.1.1  
2      *        *        *        Request timed out.  
  
10     *        *        *        Request timed out.  
11     26 ms     24 ms     31 ms     ae1...akamai.com [23.197.64.72]  
12     30 ms     29 ms     25 ms     ae1...akamai.com [23.197.64.69]  
13     5 ms      22 ms     22 ms     ae23...akamai.com [23.210.48.109]  
14     24 ms     21 ms     25 ms     10.207.32.2  
15     37 ms     21 ms     21 ms     10.207.35.19  
16     24 ms     27 ms     18 ms     10.207.6.131  
17     28 ms     22 ms     21 ms     ns2.krystal.uk [139.162.230.184]
```



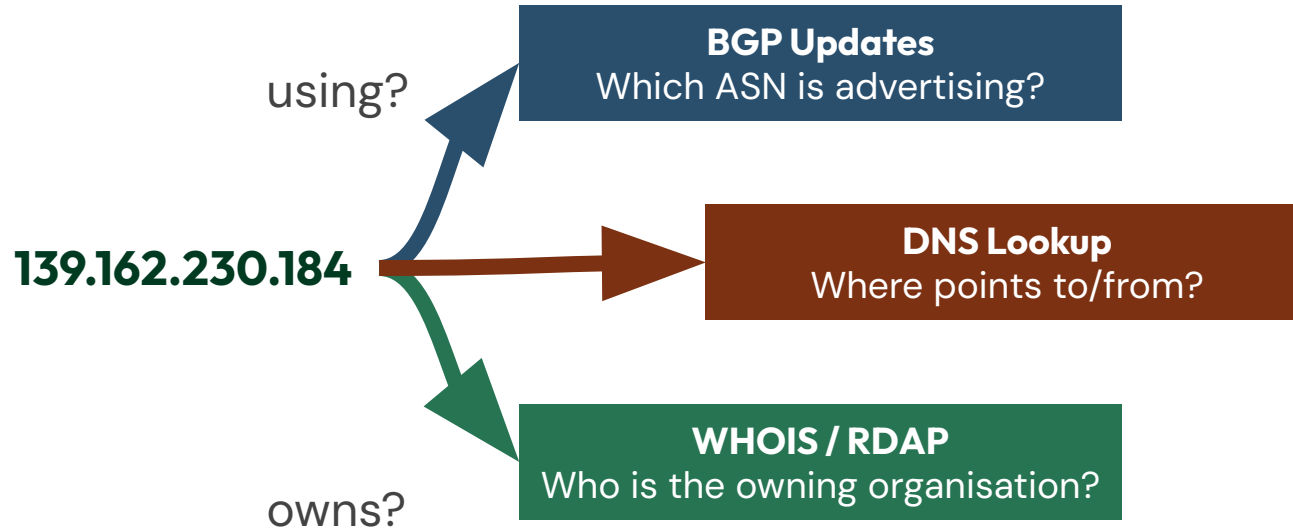
```
> traceroute  
139.162.230.184
```

**BUT THE USE ISN'T LINODE...?**

**...AND SOMEONE ELSE  
OWNS LINODE!**

```
1      2 ms      1 ms      1 ms      192.168.1.1  
2      *          *          *          Request timed out.  
3      *          *          *          Request timed out.  
4      *          *          *          Request timed out.  
5      *          *          *          Request timed out.  
6      *          *          *          Request timed out.  
7      *          *          *          Request timed out.  
8      *          *          *          Request timed out.  
9      *          *          *          Request timed out.  
10     *          *          *          Request timed out.  
11     26 ms     24 ms     31 ms     ae1...akamai.com [23.197.64.72]  
12     30 ms     29 ms     25 ms     ae1...akamai.com [23.197.64.69]  
13     35 ms     22 ms     22 ms     ae23...akamai.com [23.210.48.109]  
14     24 ms     21 ms     25 ms     10.207.32.2  
15     37 ms     21 ms     21 ms     10.207.35.19  
16     24 ms     27 ms     18 ms     10.207.6.131  
17     28 ms     22 ms     21 ms     ns2.krystal.uk [139.162.230.184]
```

# Solving the WHO



[illegible]

## 7KB response returns little actual information

Registrar  
'Krystal Hosting Ltd'  
(+ address, email)

# Solving the WHO

Inconsistent format *and*  
duplicated information

- RDAP Lookup: 139.162.230.184
  - Name: EU-LINODE-20141229
  - Entities:
    - Registrant: LINODE-MNT, ORG-LL27-RIPE, LINODE-MNT
      - Name: 'linode-mnt'
      - Name: 'Linode, LLC' (+ tel)
      - Name: 'linode-mnt'
    - Administrative: TA2589-RIPE
      - Name: (Person) (+ tel)
    - Technical: TA2589-RIPE
      - Name: (Person) (+ tel)
    - Abuse: LAS85-RIPE
      - Name: 'Linode Abuse Support' (+ email)

## Info Bank

139.162.230.184

### Registrant

'linode-mnt' (x2)

'Linode, LLC' (+ tel)

### Admin, Tech

(Person) (+ tel)

### Abuse

'Linode Abuse Support'  
(+ email)

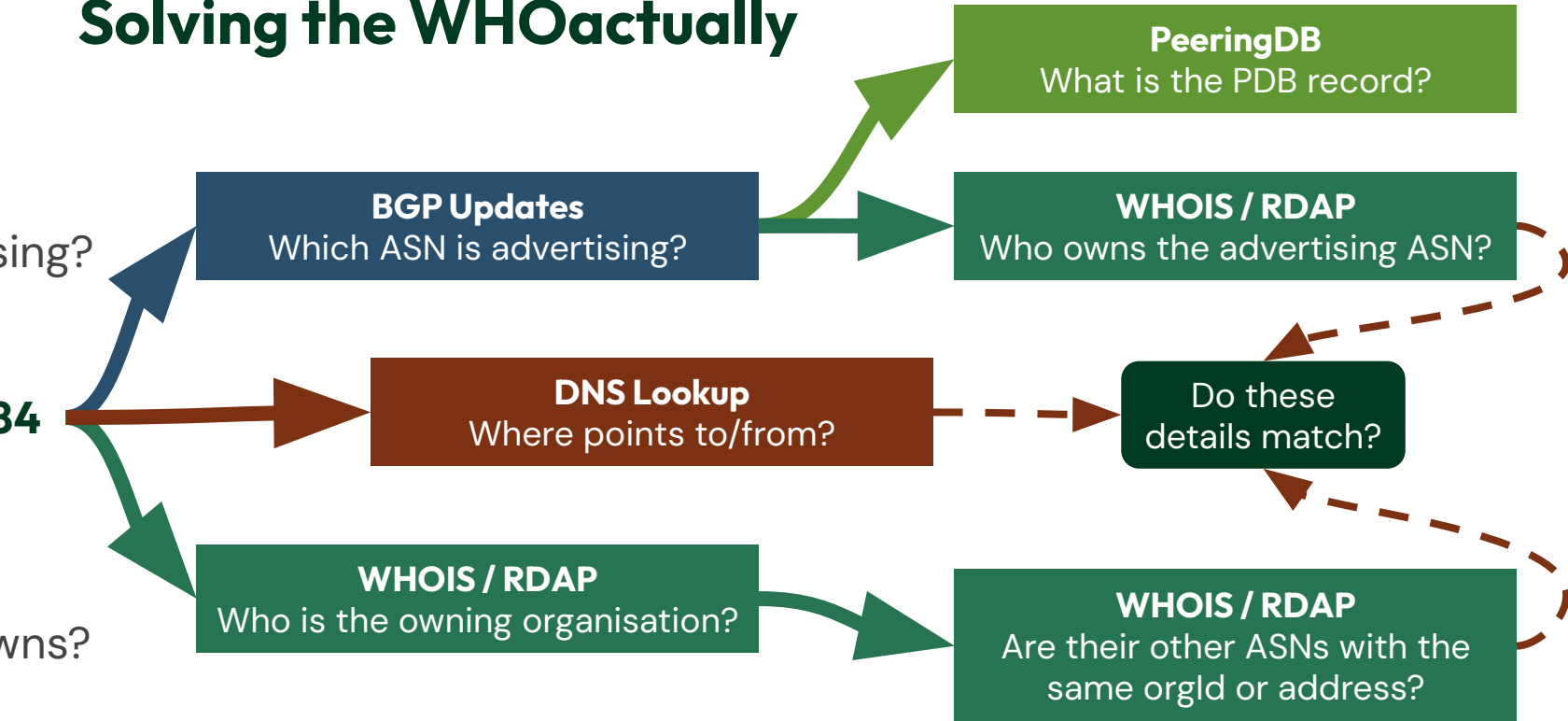
ns2.krystal.uk

krystal.uk

### Registrar

'Krystal Hosting Ltd'  
(+ address, email)

# Solving the WHO



# Matching names

1. Are the names an exact match, without punctuation?  
(Aiming for >80%)

LINODE, LLC

LINODE LLC – network administrator

2. Does a subset of the name match?  
(Aiming for >80)

LINODE, LLC

LINODE LLC – network administrator

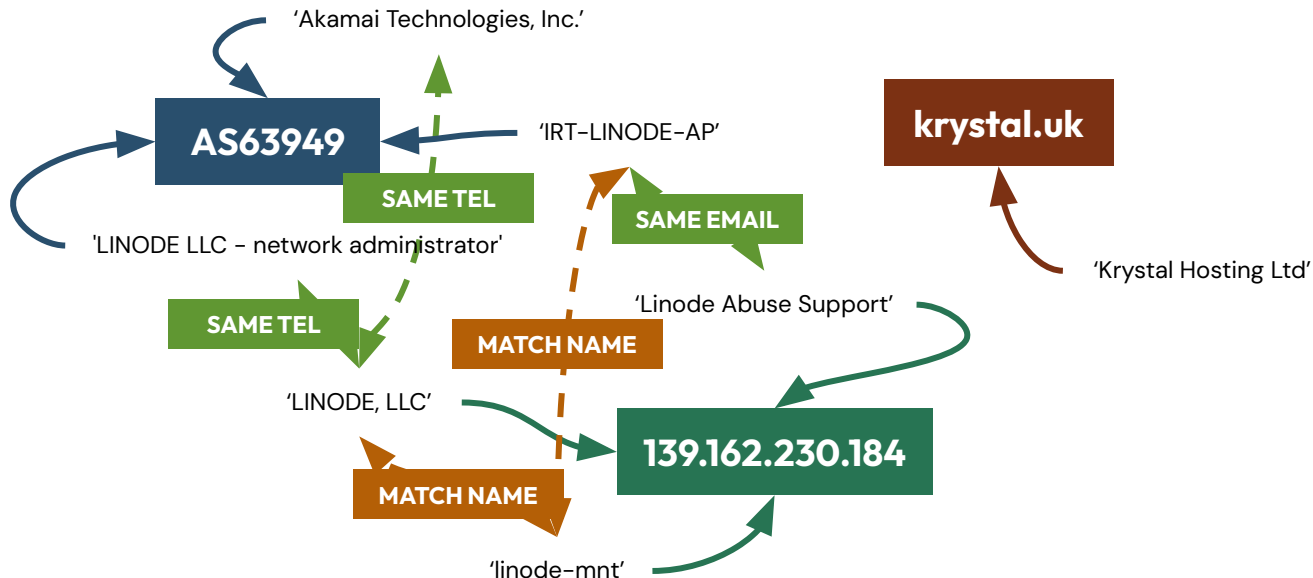
- a. What is the distance from the partial match to full match?  
(Aiming for >50)

23 (full match ratio 47%)

→ **Not a match**

# Solving the WHOactually

- Can we match any of these details?



## Info Bank

139.162.230.184

## Registrant

'linode-mnt' (x2)

'Linode, LLC' (+ tel)

## Admin, Tech

(Person) (+ tel)

## Abuse

'Linode Abuse Support'  
(+ email)

ns2.krystal.uk

krystal.uk

## Registrar

'Krystal Hosting Ltd'  
(+ address, email)

AS63949

AKAMAI-LINODE-AP

## Admin, Tech

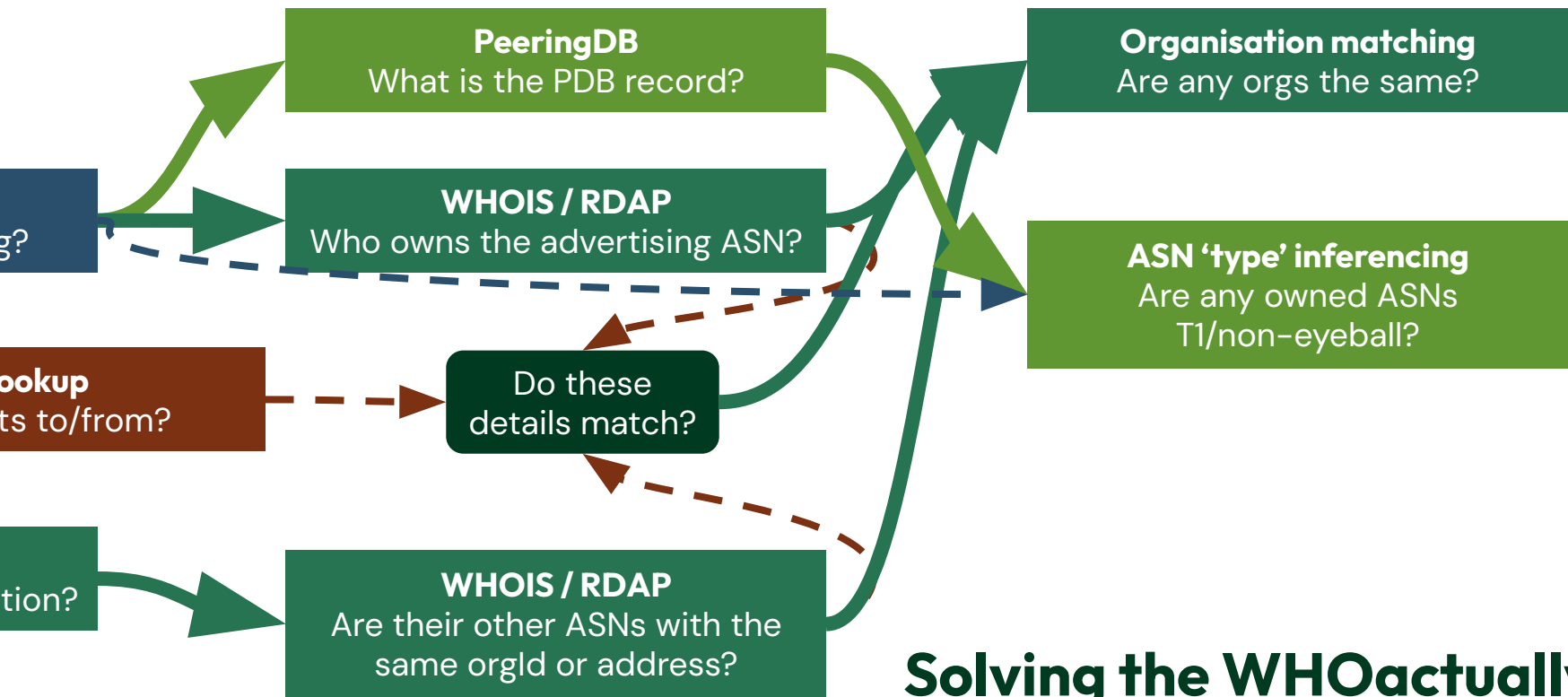
'LINODE LLC - network administrator'  
(+ tel, email)

## Registrant

'Akamai Technologies, Inc.  
(+ tel, email)

## Abuse

'IRT-LINODE-AP' (+ email)



## Solving the WHOactuallyIS

# Solving the WHOactuallyIS

What we think we know about: **139.162.230.184**

- **Owned by:**
  - 'Linode, LLC', 'linode-mnt' (from RDAP)  
Same as 'Akamai Technologies, Inc.' (from matching)
- **Operated by:**
  - 'Linode, LLC', 'linode-mnt' (from RDAP)
  - 'Krystal Hosting Ltd' (from DNS, RDAP)  
(who are not the same)

## Info Bank

139.162.230.184

### Registrant

'linode-mnt' (x2)  
'Linode, LLC' (+ tel)

### Admin, Tech

(Person) (+ tel)

### Abuse

'Linode Abuse Support'  
(+ email)

ns2.krystal.uk

krystal.uk

### Registrar

'Krystal Hosting Ltd'  
(+ address, email)

AS63949

AKAMAI-LINODE-AP

### Admin, Tech

'LINODE LLC - network  
administrator'  
(+ tel, email)

### Registrant

'Akamai Technologies, Inc.'  
(+ tel, email)

### Abuse

'IRT-LINODE-AP' (+ email)

### PeeringDB Name

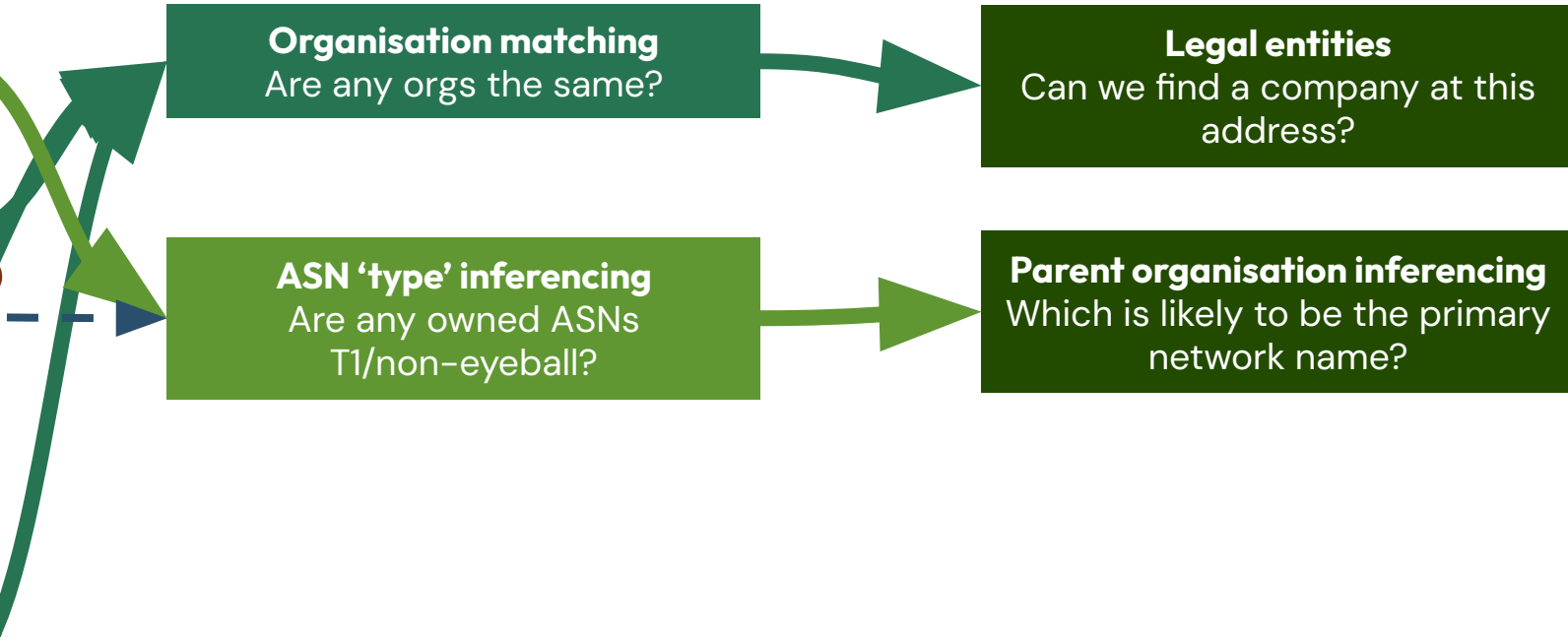
'Linode AS63949'

'Linode'

### PeeringDB Org

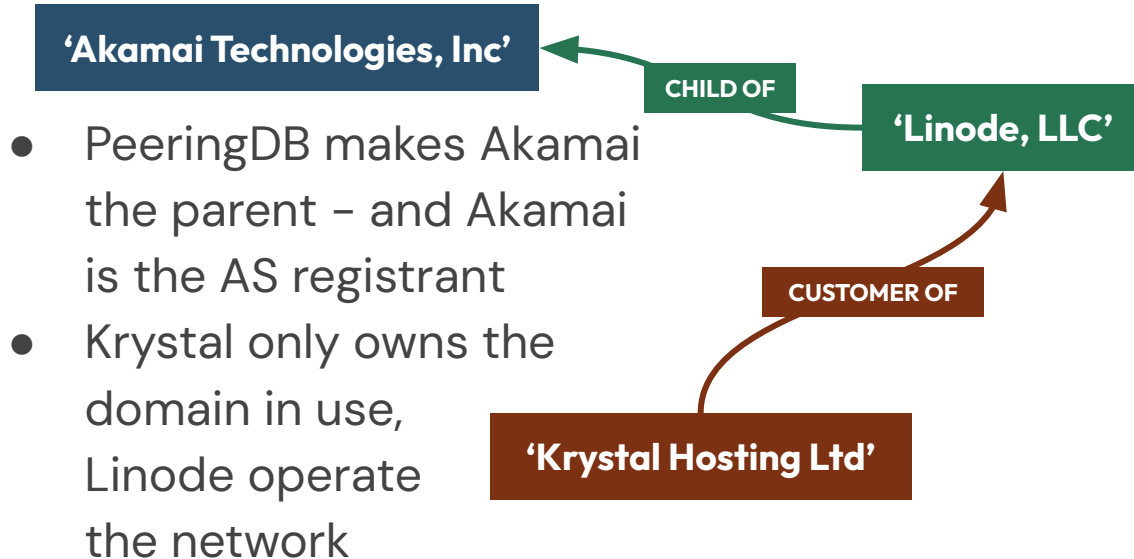
'Akamai Technologies, Inc'  
(+ address)

# Solving the WHOactuallyIS+



# Solving the WHOactuallyIS+

What we think we know about: **139.162.230.184**



## Info Bank

139.162.230.184

### Registrant

'linode-mnt' (x2)

'Linode, LLC' (+ tel)

### Admin, Tech

(Person) (+ tel)

### Abuse

'Linode Abuse Support' (+ email)

ns2.krystal.uk

krystal.uk

### Registrar

'Krystal Hosting Ltd' (+ address, email)

AS63949

AKAMAI-LINODE-AP

### Admin, Tech

'LINODE LLC – network administrator' (+ tel, email)

### Registrant

'Akamai Technologies, Inc.' (+ tel, email)

### Abuse

'IRT-LINODE-AP' (+ email)

### PeeringDB Name

'Linode AS63949'

'Linode'

### PeeringDB Org

'Akamai Technologies, Inc' (+ address)

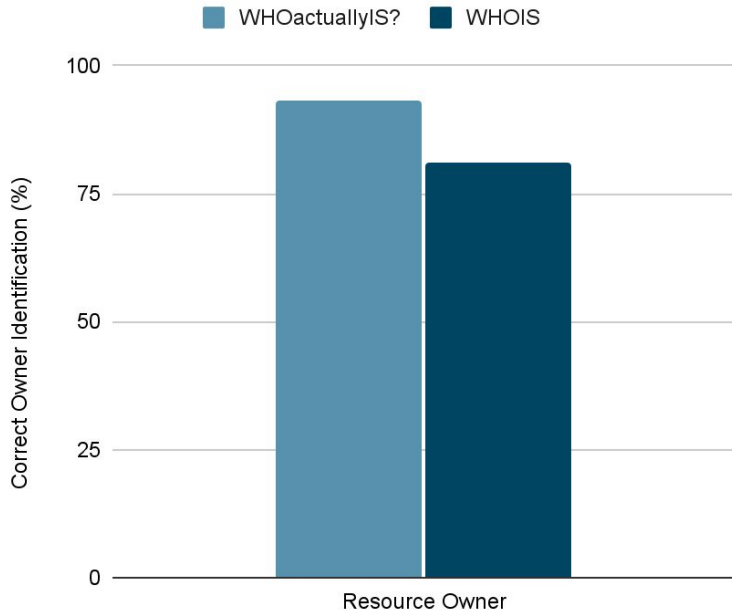
# Validation

We prepare a validation set of 200 Internet resources

- Top 100 domain names from Cloudflare's 1.1.1.1 DNS resolver list
- 50 IP addresses from RIPE Atlas traceroute destinations  
(This is likely to be biased towards network resources – helping protect end-user privacy)
- 50 highest-ranked ASNs from APNIC Eyeballs data

**There is potentially a bias towards larger companies with more connected resources – but many of them have taken active steps to obscure or withhold information.**

# Validation: Results



- WHOactuallyIS? returned the correct parent owner name for 93.1% of resources (primary name or 'aka')
- In 83.0% of cases, it returned the correct name as the primary result
- In 95.8% of cases where WHOactuallyIS? returned a result matching the manual lookup (or a subset of it).

# Summary

- WHOIS information, whilst *technically* accurate, isn't the whole truth.
- Tracking ownership across registries is **really hard**.
- Improvements can be found in traditional 'NLP' techniques.
- Try for yourself:  
 [LevettJ/who-actually-is](#)

# Questions & Contact

**SYSTRON Lab**

[systronlab.github.io](https://systronlab.github.io)

**Joshua Levett**

[joshua.levett@york.ac.uk](mailto:joshua.levett@york.ac.uk)

**GitHub**

 [LevettJ/who-actually-is](https://github.com/LevettJ/who-actually-is)