EUROPOL
EC3 European Cybercrime Centre

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

WHOIS ACCURACY AND PUBLIC SAFETY

RIPE 73
24 - 28 OCT 2016
MADRID, SPAIN

Gregory Mounier
Head of Outreach
European Cybercrime Centre (EC3)
EUROPOL

OBJECTIVES

- Public Safety Uses of WHOIS
- Current WHOIS accuracy challenges
- Case example involving inaccurate WHOIS
- Lay the ground for mutually beneficial policy on WHOIS accuracy

USES of WHOIS

Not only RIR community, but public uses of WHOIS:

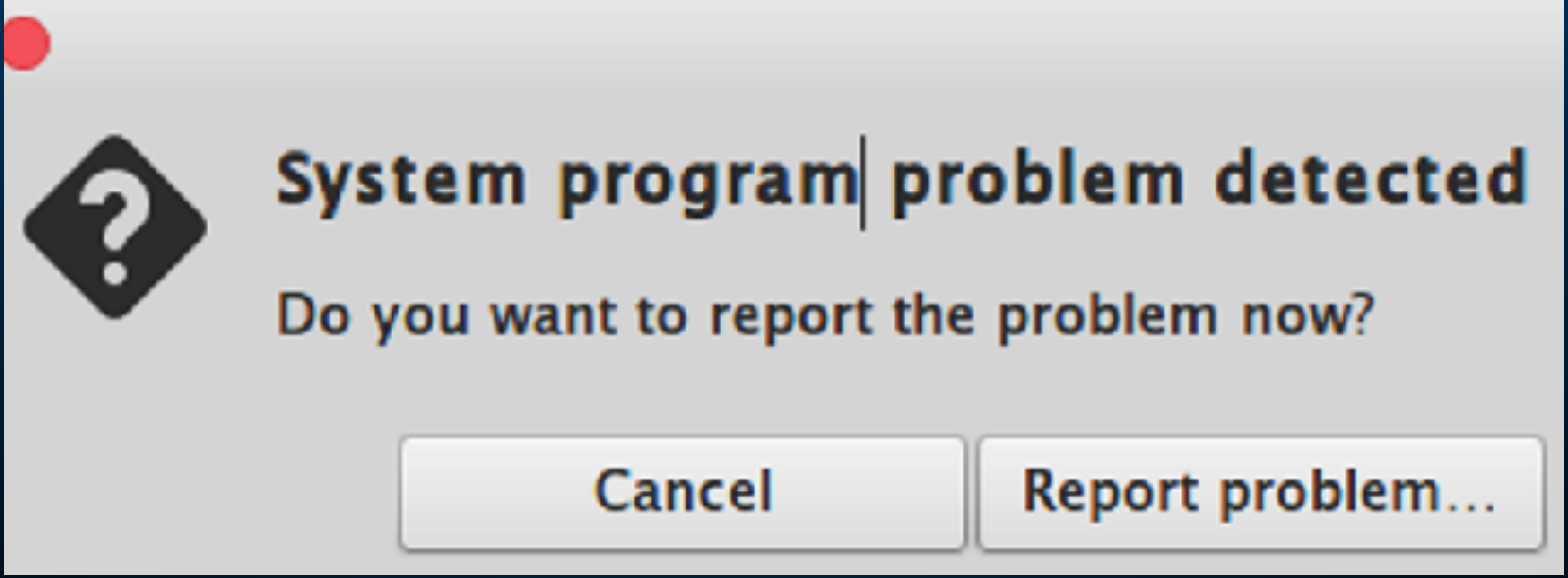
- **ACCOUNTABILITY:** Ensuring IP address holders are properly registered so individuals, consumers and the public are empowered **to resolve abusive practices that impact safety and security**
- Ensuring the **security and reliability of the network**
- Assisting businesses, consumer groups, healthcare organizations and other organizations in **combating abuse and fraud**
- Finding information about **potential bad actors using IP number resources**
- Complying with national, civil and criminal **due process** laws

PUBLIC SAFETY USE OF WHOIS

- WHOIS lookups are **one of many tools** investigators use in addition to:
  - Routing tables/services
  - Commercially available tools
  - Internally developed tools and services

- However, WHOIS is the most common **starting point** for most investigations

THE PROBLEM



System program problem detected

Do you want to report the problem now?

THE PROBLEM

- **IP Address Chain of Custody Inaccuracy Issue:**
  - Sub-allocations are not documented **to the last downstream provider** -> leads to inaccuracy
  - Each RIR tends to have different policies and requirements for what information to retain regarding sub-allocations

- **Problem only expanding as IP becomes more ubiquitous in devices**
  - IOT expansion
  - IPv6
  - IETF MODERN Protocol

- **Seeking industry solution**
  - Work with RIPE community for best solution

CHALLENGES

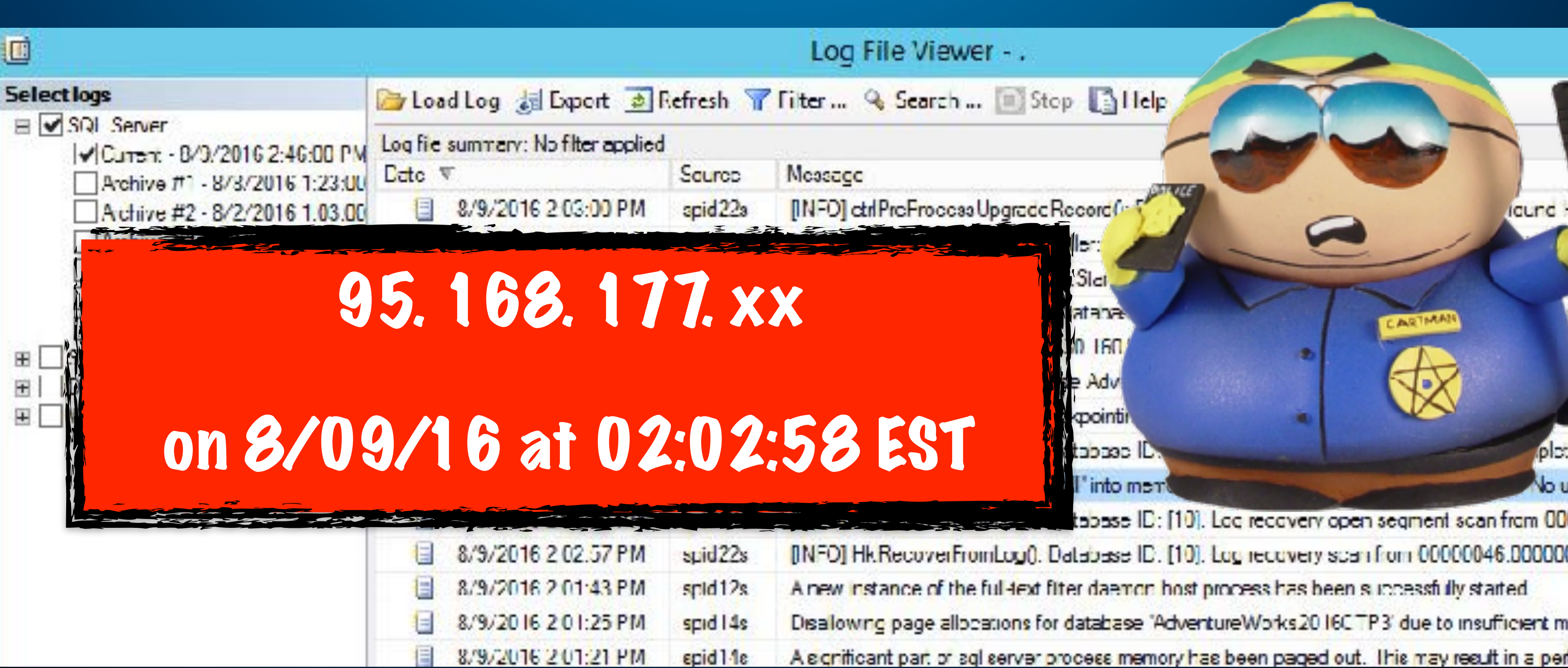
Failure to get accurate WHOIS information can present the following challenges:

- Inability to quickly identify resources used in abusive activities
- Inability to serve legal process to the party responsible for the resources - finding jurisdiction for suspects & victims
- Waste of time of investigators and network operators: Investigators go from ISP to ISP to serve legal notice
- More abuse: IP hijacking…

CASE STUDY

POLICE
CARTMAN
PRICE CUT

7.8 Million customer details



Select logs

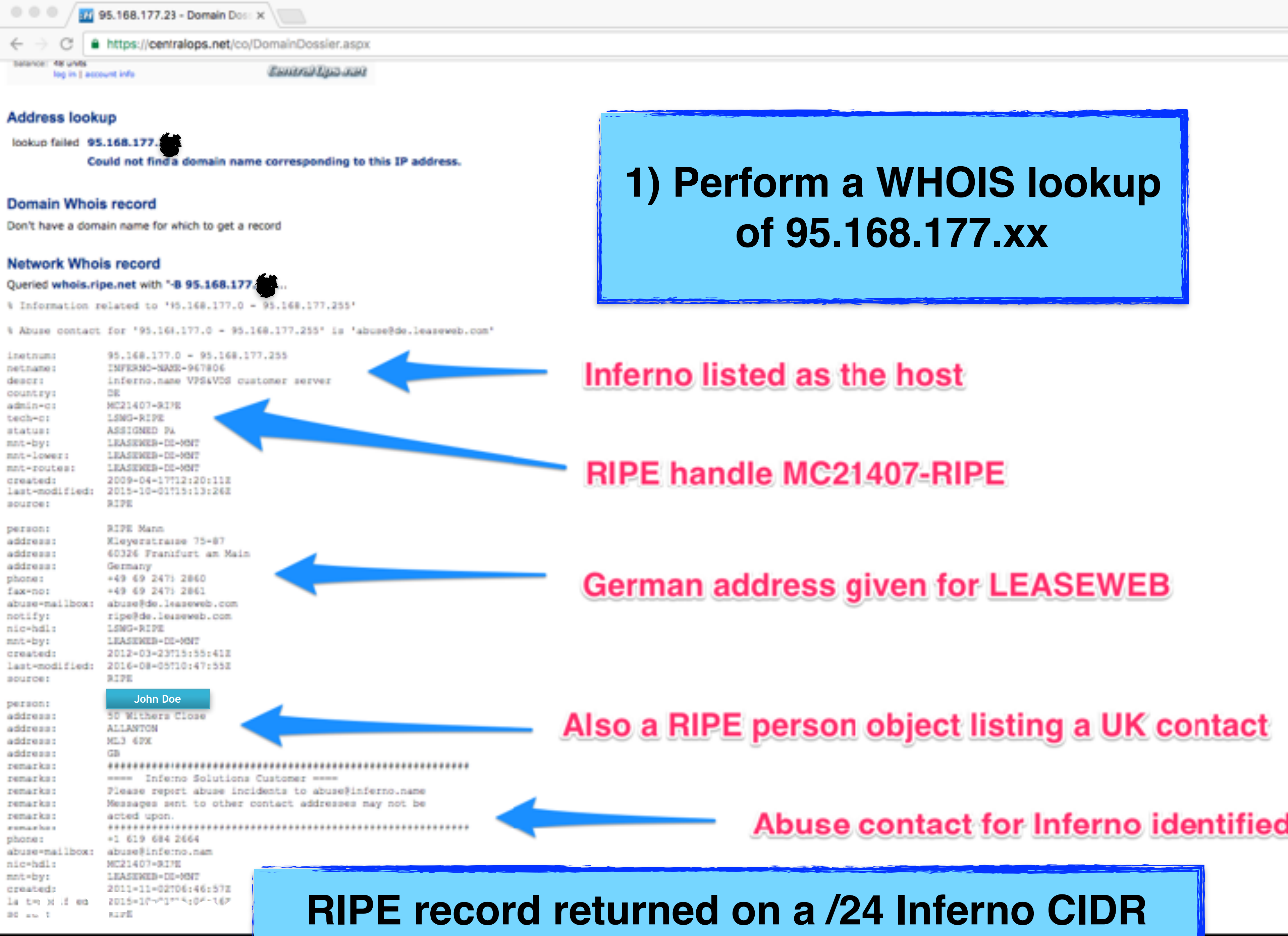
- ☑ SQL Server
  - ☑ Current - 8/9/2016 2:46:00 PM
  - □ Archive #1 - 8/3/2016 1:23:00
  - □ Archive #2 - 8/2/2016 1:03:00

Log file summary: No filter applied

```
Date                   Source    Message
8/9/2016 2:03:00 PM    spid22s   [INFO] ctrlProProcessUpgradeRecord(
                                 tabase ID: [10]. Log recovery open segment scan from 00
8/9/2016 2:02:57 PM    spid22s   [INFO] HkRecoverFromLog(). Database ID: [10]. Log recovery scan from 0000046.00000
8/9/2016 2:01:43 PM    spid12s   A new instance of the full-text filter daemon host process has been successfully started
8/9/2016 2:01:25 PM    spid14s   Disallowing page allocations for database 'AdventureWorks2016CTP3' due to insufficient m
8/9/2016 2:01:21 PM    spid11s   A significant part of sql server process memory has been paged out. This may result in a per
```

95.168.177.xx

on 8/09/16 at 02:02:58 EST



95.168.177.23 - Domain Dos
https://centralops.net/co/DomainDossier.aspx
balance: 48 units
log in | account info
CentralOps.net

1) Perform a WHOIS lookup of 95.168.177.xx

Address lookup

lookup failed **95.168.177.**[redacted]

Could not find a domain name corresponding to this IP address.

Domain Whois record

Don't have a domain name for which to get a record

Network Whois record

Queried **whois.ripe.net** with "-B **95.168.177.**[redacted]..."

```
% Information related to '95.168.177.0 - 95.168.177.255'

% Abuse contact for '95.168.177.0 - 95.168.177.255' is 'abuse@de.leaseweb.com'

inetnum:        95.168.177.0 - 95.168.177.255
netname:        INFERNO-NAME-967806
descr:          inferno.name VPS&VDS customer server
country:        DE
admin-c:        MC21407-RIPE
tech-c:         LSWG-RIPE
status:         ASSIGNED PA
mnt-by:         LEASEWEB-DE-MNT
mnt-lower:      LEASEWEB-DE-MNT
mnt-routes:     LEASEWEB-DE-MNT
created:        2009-04-17T12:20:11Z
last-modified:  2015-10-01T15:13:26Z
source:         RIPE

person:         RIPE Mann
address:        Kleyerstrasse 75-87
address:        60326 Frankfurt am Main
address:        Germany
phone:          +49 69 2475 2860
fax-no:         +49 69 2475 2861
abuse-mailbox:  abuse@de.leaseweb.com
notify:         ripe@de.leaseweb.com
nic-hdl:        LSWG-RIPE
mnt-by:         LEASEWEB-DE-MNT
created:        2012-03-23T15:55:41Z
last-modified:  2016-08-05T10:47:55Z
source:         RIPE

person:         John Doe
address:        50 Withers Close
address:        ALLANTON
address:        ML3 6PX
address:        GB
remarks:        #################################################################
remarks:        ====  Inferno Solutions Customer ====
remarks:        Please report abuse incidents to abuse@inferno.name
remarks:        Messages sent to other contact addresses may not be
remarks:        acted upon.
remarks:        #################################################################
phone:          +1 619 684 2664
abuse-mailbox:  abuse@inferno.nam
nic-hdl:        MC21407-RIPE
mnt-by:         LEASEWEB-DE-MNT
created:        2011-11-02T06:46:57Z
last-modified:  2015-10-[illegible]:06:16Z
source:         RIPE
```

Inferno listed as the host

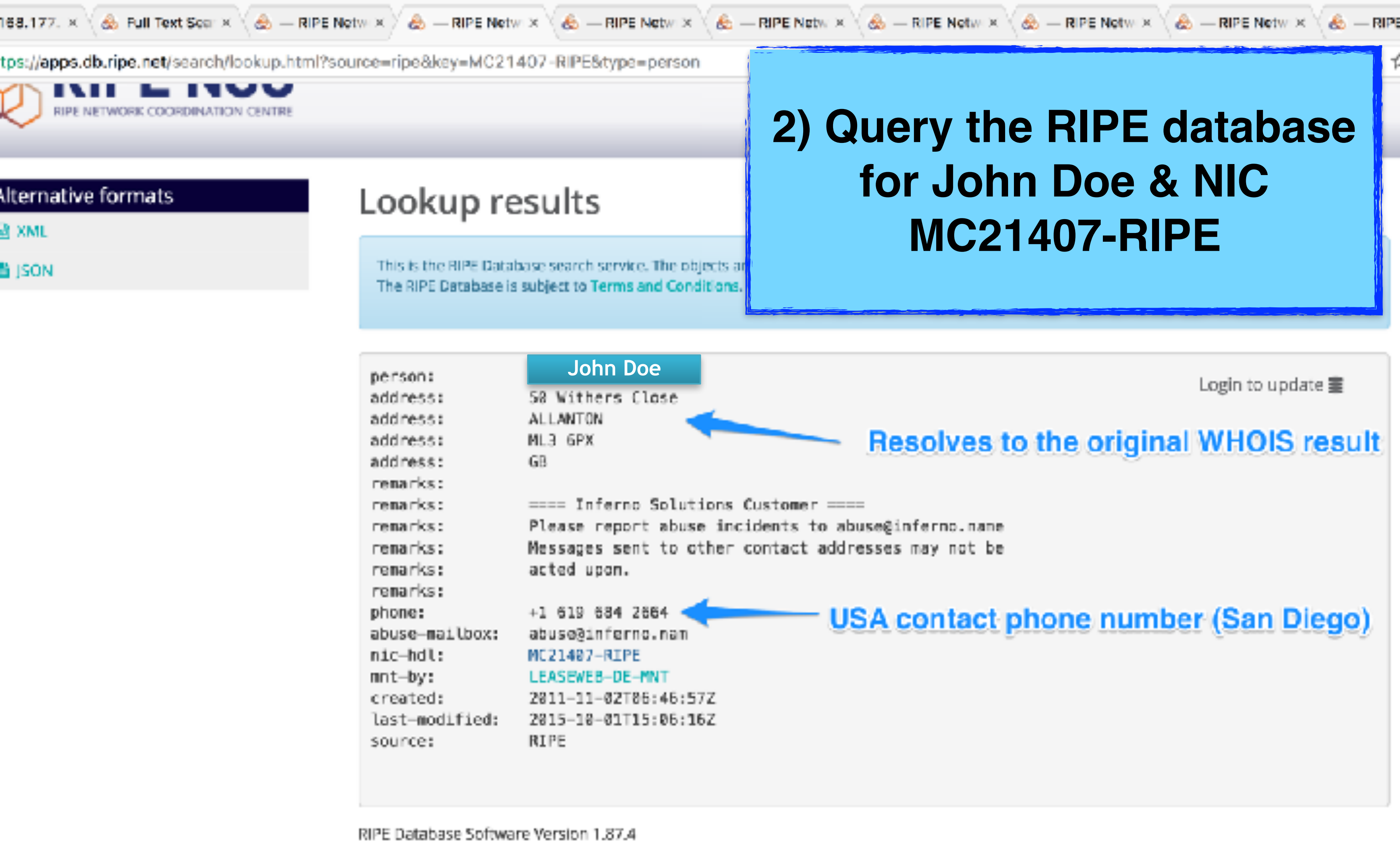
RIPE handle MC21407-RIPE

German address given for LEASEWEB

Also a RIPE person object listing a UK contact

Abuse contact for Inferno identified

RIPE record returned on a /24 Inferno CIDR



tps://apps.db.ripe.net/search/lookup.html?source=ripe&key=MC21407-RIPE&type=person

2) Query the RIPE database for John Doe & NIC MC21407-RIPE

Lookup results

This is the RIPE Database search service. The objects ar
The RIPE Database is subject to Terms and Conditions.

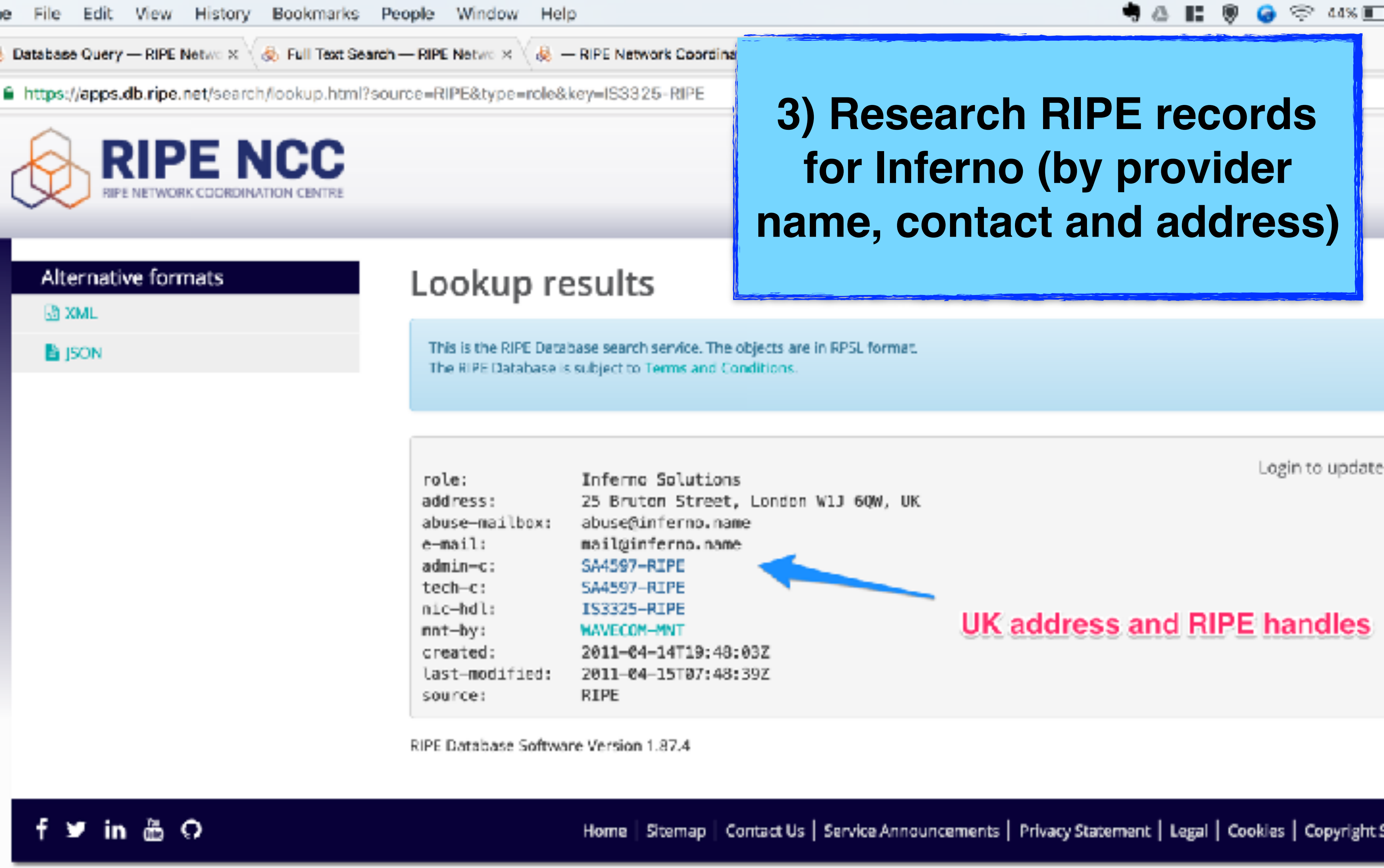
```
person:          John Doe
address:         58 Withers Close
address:         ALLANTON
address:         ML3 6PX
address:         GB
remarks:
remarks:         ==== Inferno Solutions Customer ====
remarks:         Please report abuse incidents to abuse@inferno.name
remarks:         Messages sent to other contact addresses may not be
remarks:         acted upon.
remarks:
phone:           +1 619 684 2864
abuse-mailbox:   abuse@inferno.nam
nic-hdl:         MC21407-RIPE
mnt-by:          LEASEWEB-DE-MNT
created:         2011-11-02T06:46:57Z
last-modified:   2015-10-01T15:06:16Z
source:          RIPE
```

Resolves to the original WHOIS result

USA contact phone number (San Diego)

RIPE Database Software Version 1.87.4

3) Research RIPE records for Inferno (by provider name, contact and address)


File Edit View History Bookmarks People Window Help
Database Query — RIPE Netw
Full Text Search — RIPE Netw
— RIPE Network Coordina
https://apps.db.ripe.net/search/lookup.html?source=RIPE&type=role&key=IS3325-RIPE
RIPE NCC
RIPE NETWORK COORDINATION CENTRE
Alternative formats
XML
JSON
Login to update
Home | Sitemap | Contact Us | Service Announcements | Privacy Statement | Legal | Cookies | Copyright

Lookup results

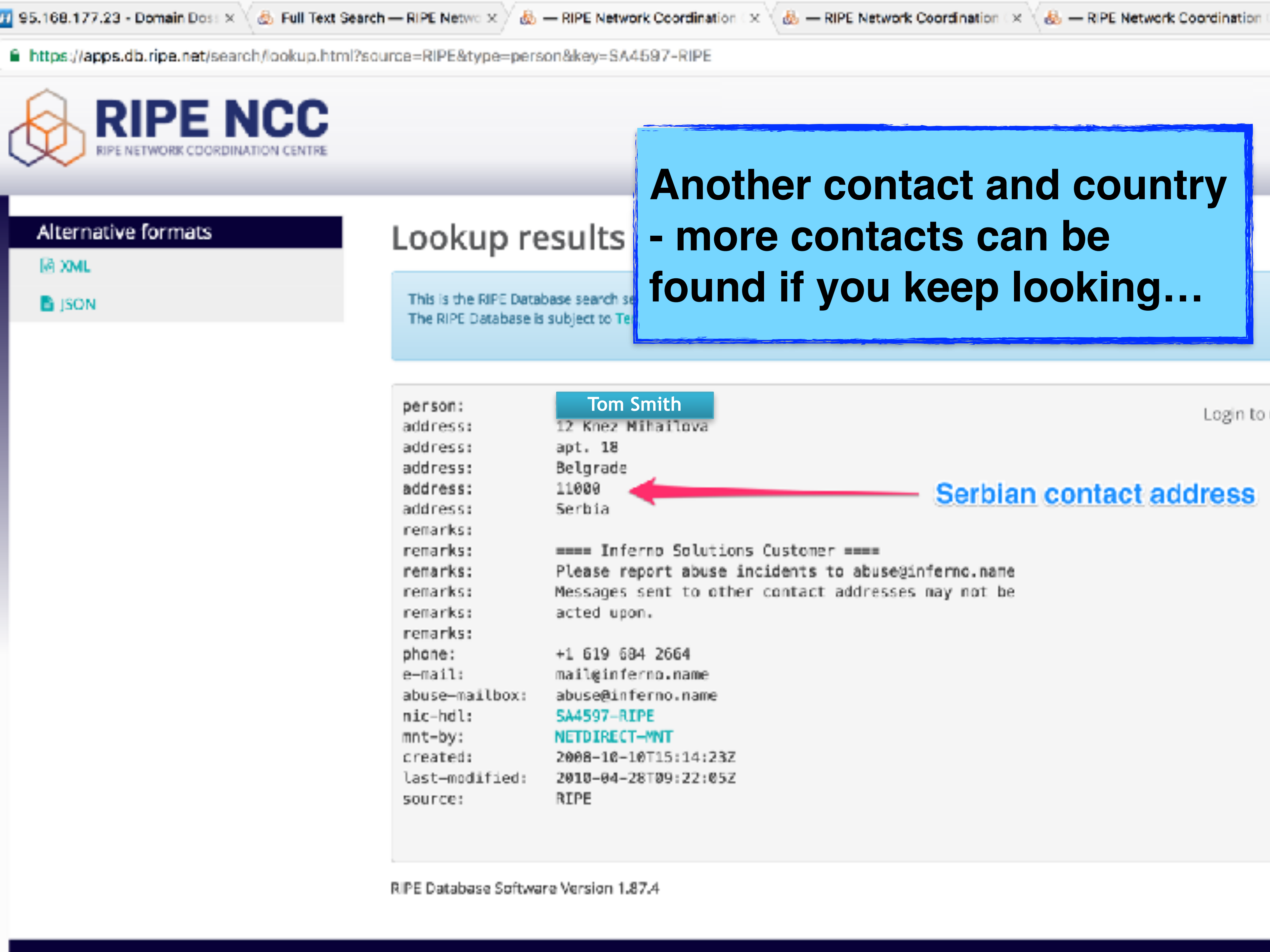
This is the RIPE Database search service. The objects are in RPSL format.
The RIPE Database is subject to Terms and Conditions.

```
role:           Inferno Solutions
address:        25 Bruton Street, London W1J 6QW, UK
abuse-mailbox:  abuse@inferno.name
e-mail:         mail@inferno.name
admin-c:        SA4597-RIPE
tech-c:         SA4597-RIPE
nic-hdl:        IS3325-RIPE
mnt-by:         WAVECOM-MNT
created:        2011-04-14T19:48:03Z
last-modified:  2011-04-15T07:48:39Z
source:         RIPE
```

UK address and RIPE handles

RIPE Database Software Version 1.87.4

Another contact and country - more contacts can be found if you keep looking…


95.168.177.23 - Domain Dos
Full Text Search — RIPE Netw
— RIPE Network Coordination
— RIPE Network Coordination
— RIPE Network Coordination
https://apps.db.ripe.net/search/lookup.html?source=RIPE&type=person&key=SA4597-RIPE
RIPE NCC
RIPE NETWORK COORDINATION CENTRE
Alternative formats
XML
JSON
Login to

Lookup results

This is the RIPE Database search se
The RIPE Database is subject to Te

```
person:         Tom Smith
address:        12 Knez Mihailova
address:        apt. 18
address:        Belgrade
address:        11000
address:        Serbia
remarks:
remarks:        ==== Inferno Solutions Customer ====
remarks:        Please report abuse incidents to abuse@inferno.name
remarks:        Messages sent to other contact addresses may not be
remarks:        acted upon.
remarks:
phone:          +1 619 684 2664
e-mail:         mail@inferno.name
abuse-mailbox:  abuse@inferno.name
nic-hdl:        SA4597-RIPE
mnt-by:         NETDIRECT-MNT
created:        2008-10-10T15:14:23Z
last-modified:  2010-04-28T09:22:05Z
source:         RIPE
```

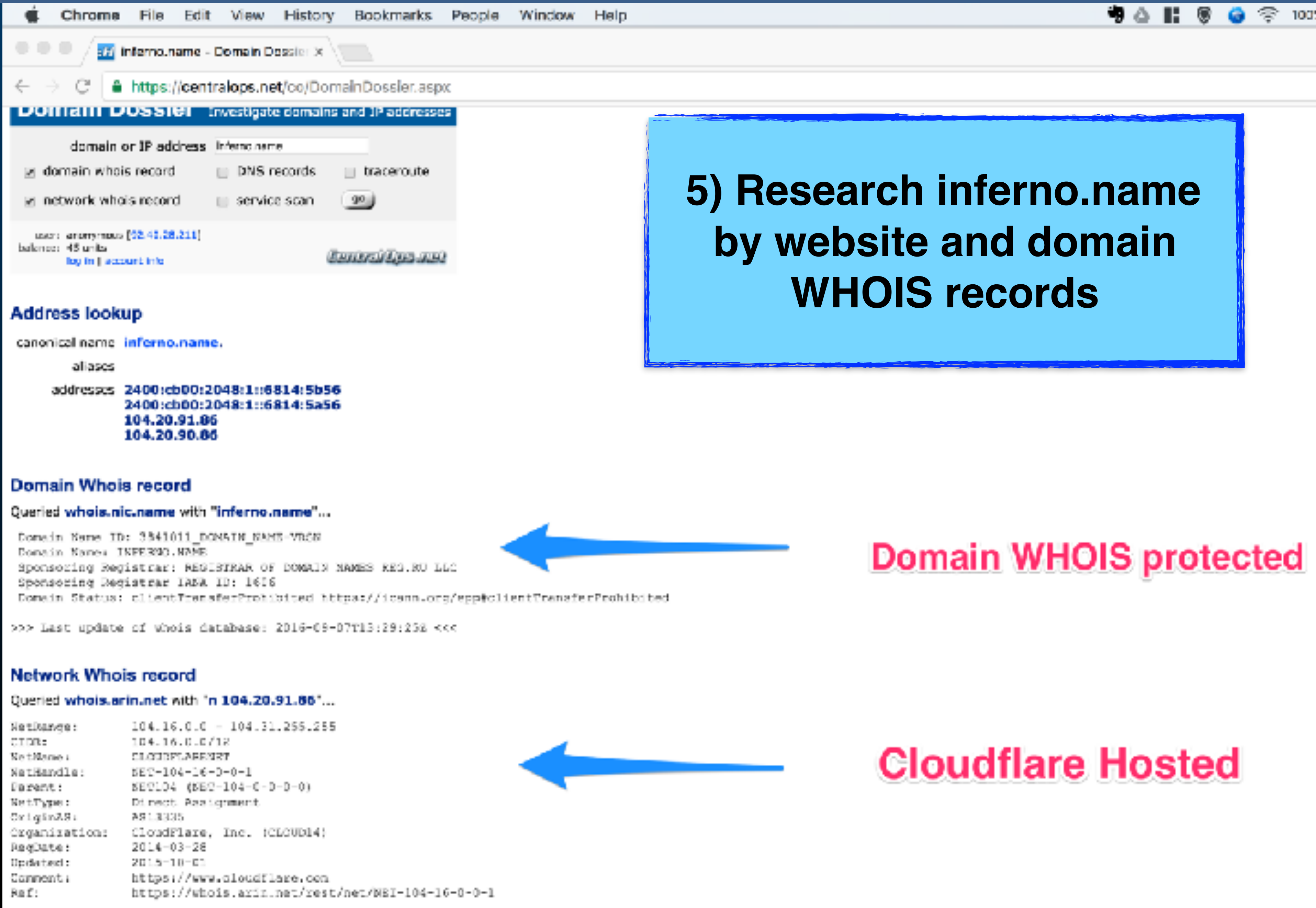
Serbian contact address

RIPE Database Software Version 1.87.4

4) Identify Inferno RIPE member records for the registered address to serve legal process on

2 person objects
2 UK addresses
1 Serbian Address
1 US contact phone number

5) Research inferno.name by website and domain WHOIS records


Chrome
File
Edit
View
History
Bookmarks
People
Window
Help
100
inferno.name - Domain Dossier ×
https://centralops.net/co/DomainDossier.aspx
Domain Dossier Investigate domains and IP addresses
CentralOps.net

domain or IP address inferno.name

☑ domain whois record □ DNS records □ traceroute
☑ network whois record □ service scan go

user: anonymous [52.41.28.211]
balance: 48 units
log in | account info

Address lookup

canonical name inferno.name.
aliases
addresses 2400:cb00:2048:1::6814:5b56
2400:cb00:2048:1::6814:5a56
104.20.91.86
104.20.90.86

Domain Whois record

Queried whois.nic.name with "inferno.name"...

```
Domain Name ID: 3341011_DOMAIN_NAME-VRSN
Domain Name: INFERNO.NAME
Sponsoring Registrar: REGISTRAR OF DOMAIN NAMES REG.RU LLC
Sponsoring Registrar IANA ID: 1606
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

>>> Last update of whois database: 2016-09-07T13:29:23Z <<<
```

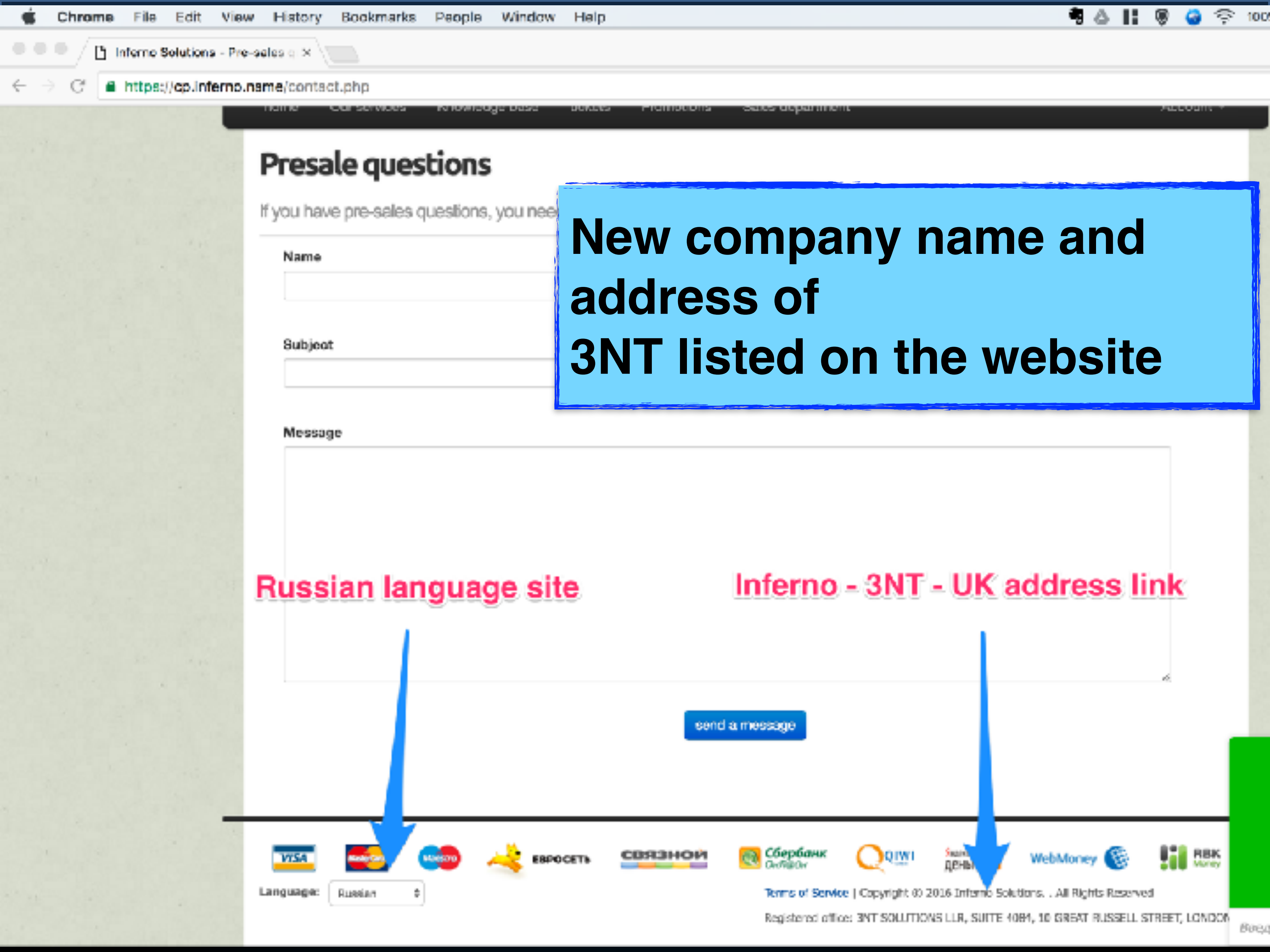
Domain WHOIS protected

Network Whois record

Queried whois.arin.net with "n 104.20.91.86"...

```
NetRange:       104.16.0.0 - 104.31.255.255
CIDR:           104.16.0.0/12
NetName:        CLOUDFLARENET
NetHandle:      NET-104-16-0-0-1
Parent:         NET104 (NET-104-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS13335
Organization:   CloudFlare, Inc. (CLOUD14)
RegDate:        2014-03-28
Updated:        2015-10-07
Comment:        https://www.cloudflare.com
Ref:            https://whois.arin.net/rest/net/NET-104-16-0-0-1
```

Cloudflare Hosted



Chrome File Edit View History Bookmarks People Window Help
Inferno Solutions - Pre-sales
https://cp.inferno.name/contact.php
send a message
Language: Russian
ЕВРОСЕТЬ
СВЯЗНОЙ
Сбербанк
QIWI
WebMoney
RBK Money

Presale questions

If you have pre-sales questions, you nee

Name

Subject

Message

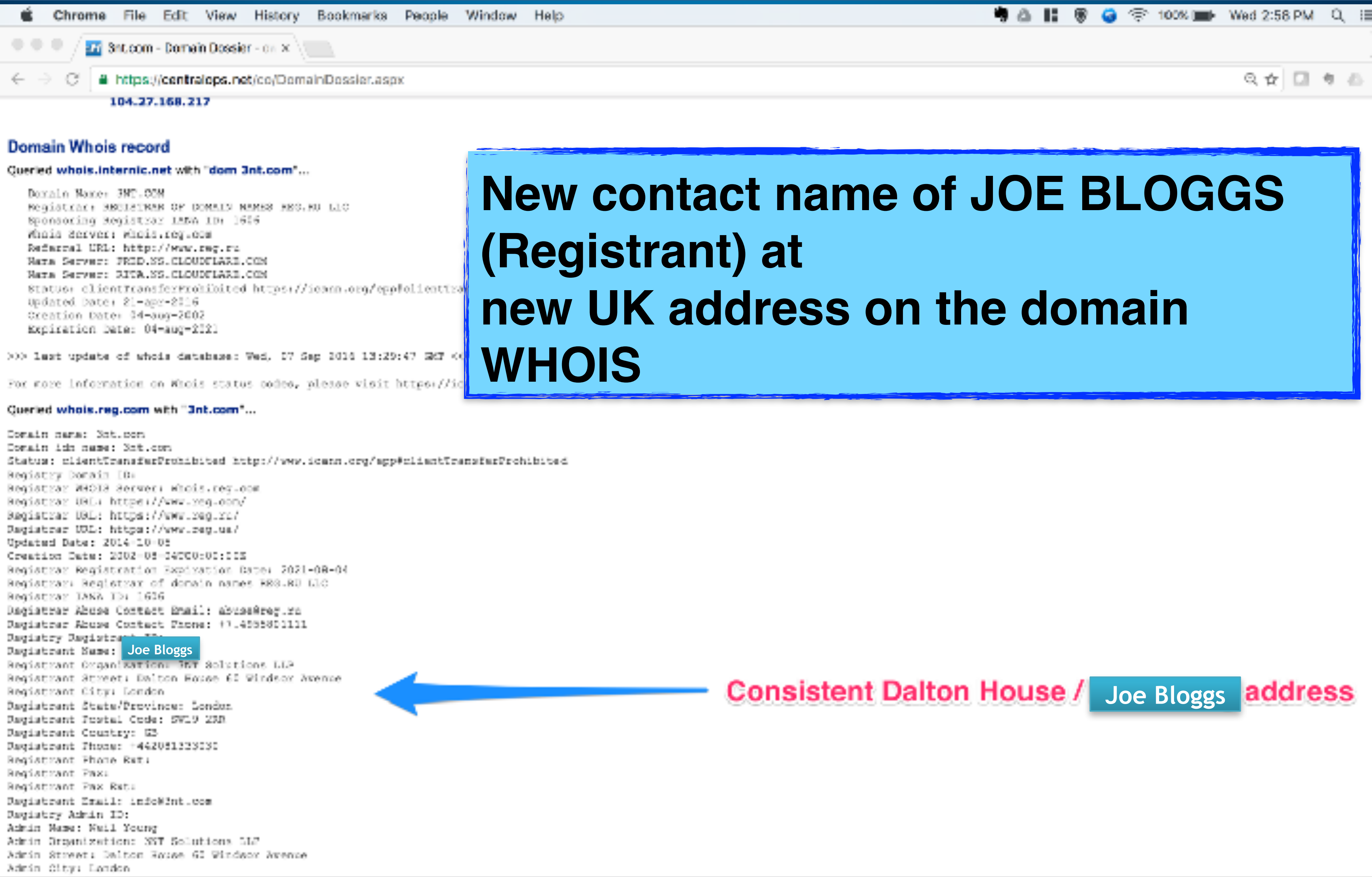
New company name and address of 3NT listed on the website

Russian language site

Inferno - 3NT - UK address link

Terms of Service | Copyright © 2016 Inferno Solutions. . All Rights Reserved

Registered office: 3NT SOLUTIONS LLP, SUITE 4084, 10 GREAT RUSSELL STREET, LONDON


Chrome
File
Edit
View
History
Bookmarks
People
Window
Help
100%
Wed 2:58 PM
3nt.com - Domain Dossier - ce
https://centralops.net/co/DomainDossier.aspx

104.27.168.217

Domain Whois record

Queried **whois.internic.net** with "**dom 3nt.com**"...

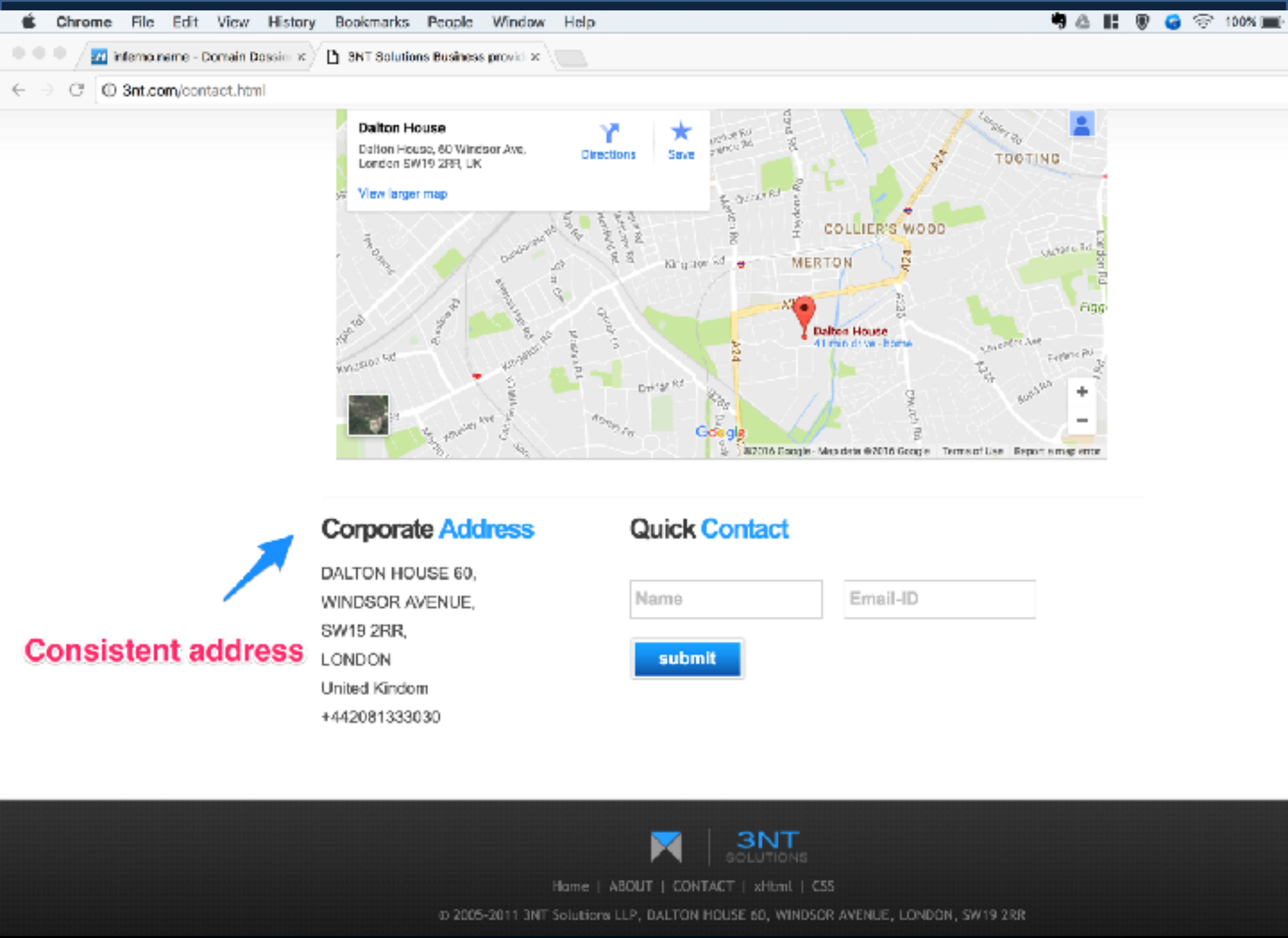
```
   Domain Name: 3NT.COM
   Registrar: REGISTRAR OF DOMAIN NAMES REG.RU LLC
   Sponsoring Registrar IANA ID: 1606
   Whois Server: whois.reg.com
   Referral URL: http://www.reg.ru
   Name Server: FRED.NS.CLOUDFLARE.COM
   Name Server: RITA.NS.CLOUDFLARE.COM
   Status: clientTransferProhibited https://icann.org/epp#clienttra
   Updated Date: 21-apr-2016
   Creation Date: 04-aug-2002
   Expiration Date: 04-aug-2021

>>> Last update of whois database: Wed, 07 Sep 2016 13:29:47 GMT <<

For more information on Whois status codes, please visit https://ic
```

Queried **whois.reg.com** with "**3nt.com**"...

```
Domain name: 3nt.com
Domain idn name: 3nt.com
Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Domain ID:
Registrar WHOIS Server: whois.reg.com
Registrar URL: https://www.reg.com/
Registrar URL: https://www.reg.ru/
Registrar URL: https://www.reg.ua/
Updated Date: 2014-10-05
Creation Date: 2002-08-04T00:00:00Z
Registrar Registration Expiration Date: 2021-08-04
Registrar: Registrar of domain names REG.RU LLC
Registrar IANA ID: 1606
Registrar Abuse Contact Email: abuse@reg.ru
Registrar Abuse Contact Phone: +7.4955801111
Registry Registrant ID:
Registrant Name: Joe Bloggs
Registrant Organization: 3NT Solutions LLP
Registrant Street: Dalton House 60 Windsor Avenue
Registrant City: London
Registrant State/Province: London
Registrant Postal Code: SW19 2RR
Registrant Country: GB
Registrant Phone: +442081233232
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: info@3nt.com
Registry Admin ID:
Admin Name: Neil Young
Admin Organization: 3NT Solutions LLP
Admin Street: Dalton House 60 Windsor Avenue
Admin City: London
```

New contact name of JOE BLOGGS (Registrant) at new UK address on the domain WHOIS

Consistent Dalton House / Joe Bloggs address



Dalton House

Dalton House, 60 Windsor Ave,
London SW19 2RR, UK

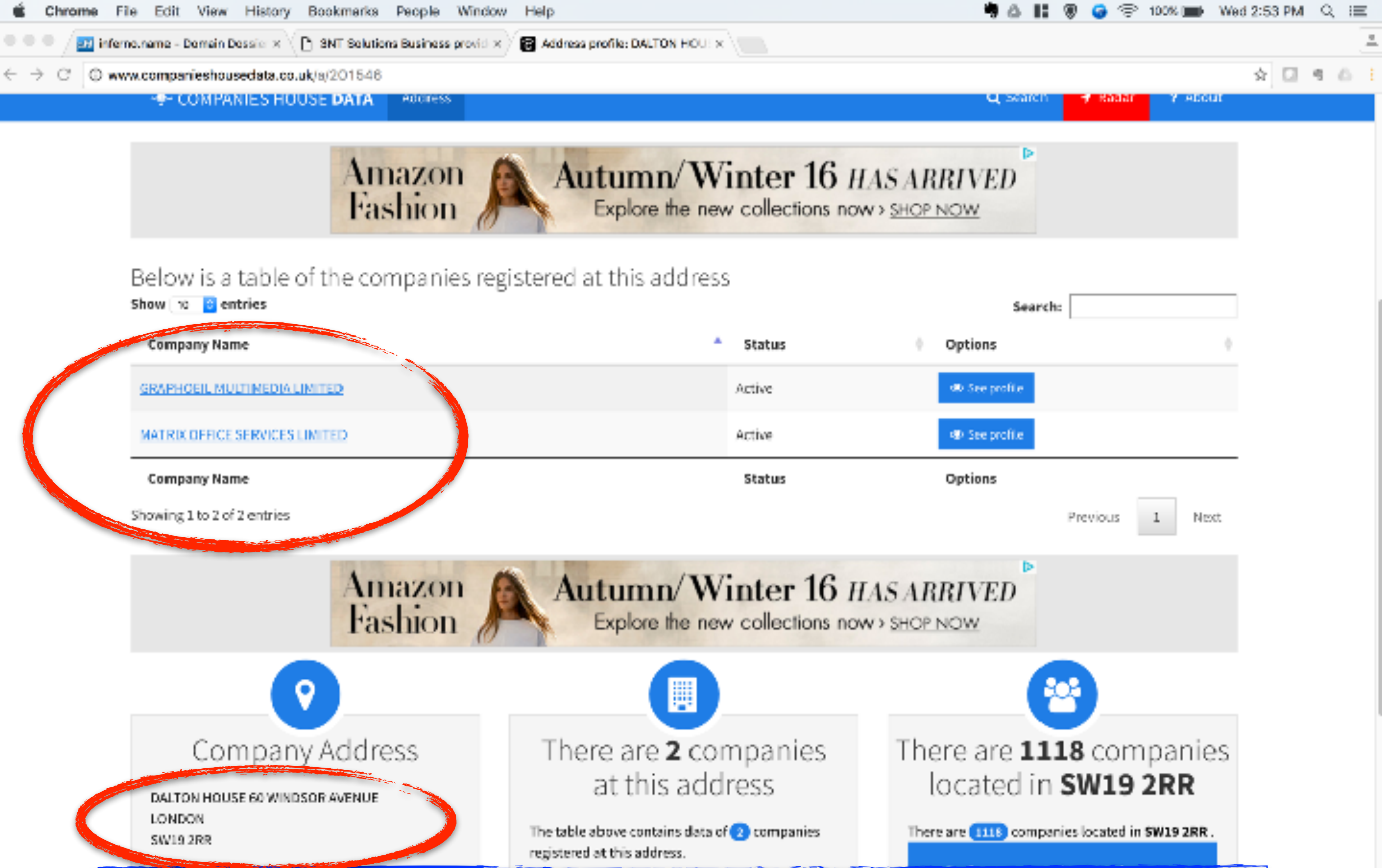
Corporate Address

DALTON HOUSE 60,
WINDSOR AVENUE,
SW19 2RR,
LONDON
United Kindom
+442081333030

Quick Contact

© 2005-2011 3NT Solutions LLP, DALTON HOUSE 60, WINDSOR AVENUE, LONDON, SW19 2RR

Consistent address


Chrome File Edit View History Bookmarks People Window Help
100% Wed 2:53 PM
inferno.name - Domain Dossie
3NT Solutions Business provid
Address profile: DALTON HOU
www.companieshousedata.co.uk/a/201546
COMPANIES HOUSE DATA
Address
Search
Radar
About

Below is a table of the companies registered at this address

Show 10 entries Search:

Company Name	Status	Options
GRAPHOEIL MULTIMEDIA LIMITED	Active	See profile
MATRIX OFFICE SERVICES LIMITED	Active	See profile
Company Name	Status	Options

Showing 1 to 2 of 2 entries

Previous 1 Next

Company Address

DALTON HOUSE 60 WINDSOR AVENUE
LONDON
SW19 2RR

There are **2** companies at this address

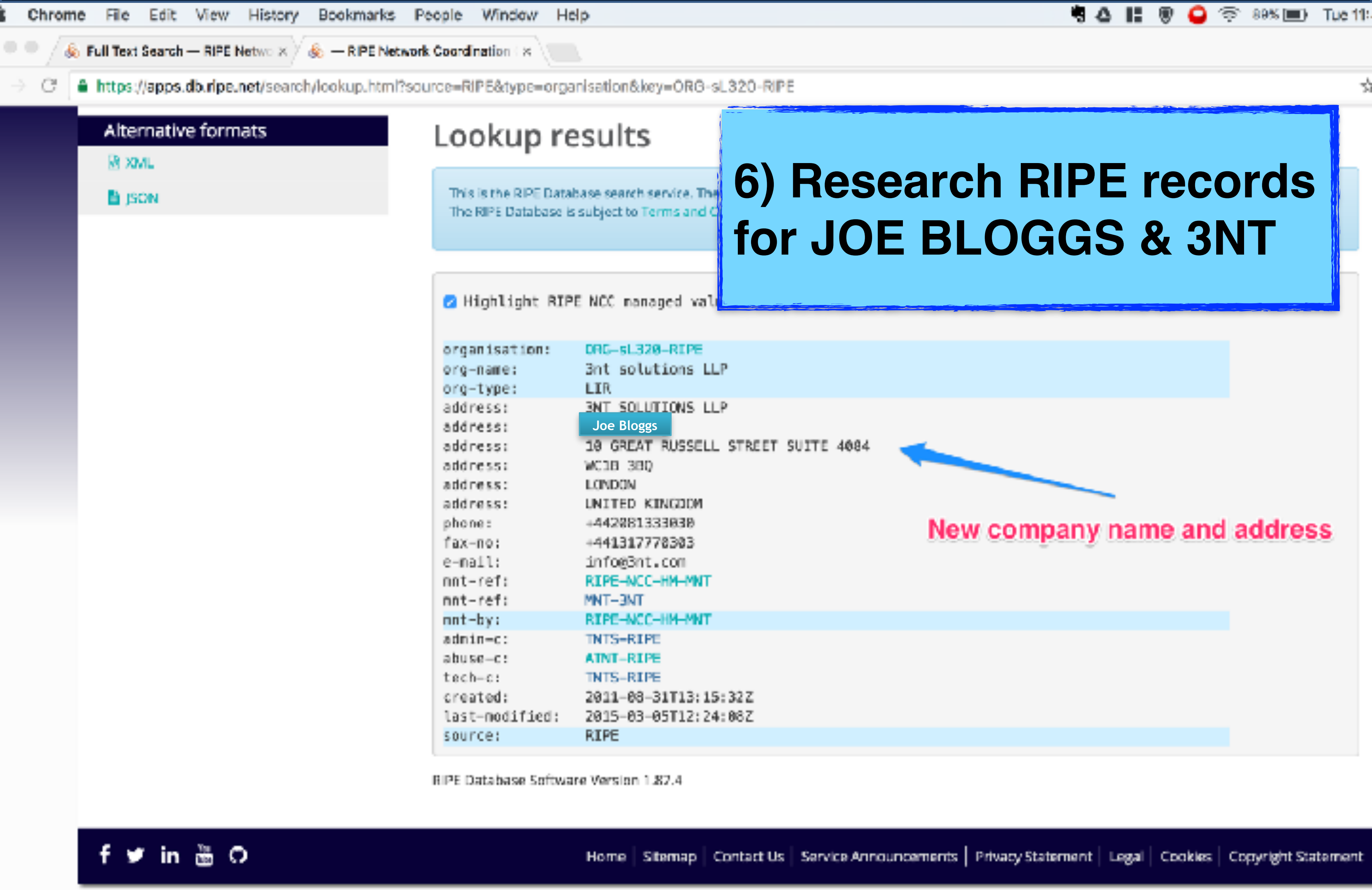
The table above contains data of 2 companies registered at this address.

There are **1118** companies located in **SW19 2RR**

There are 1118 companies located in **SW19 2RR**.

Despite listing Dalton House as a 3NT listed address they are not officially registered there

6) Research RIPE records for JOE BLOGGS & 3NT


Chrome File Edit View History Bookmarks People Window Help
Full Text Search — RIPE Netwo
— RIPE Network Coordination
https://apps.db.ripe.net/search/lookup.html?source=RIPE&type=organisation&key=ORG-sL320-RIPE
Alternative formats
XML
JSON
Home | Sitemap | Contact Us | Service Announcements | Privacy Statement | Legal | Cookies | Copyright Statement

Lookup results

This is the RIPE Database search service. The
The RIPE Database is subject to Terms and C

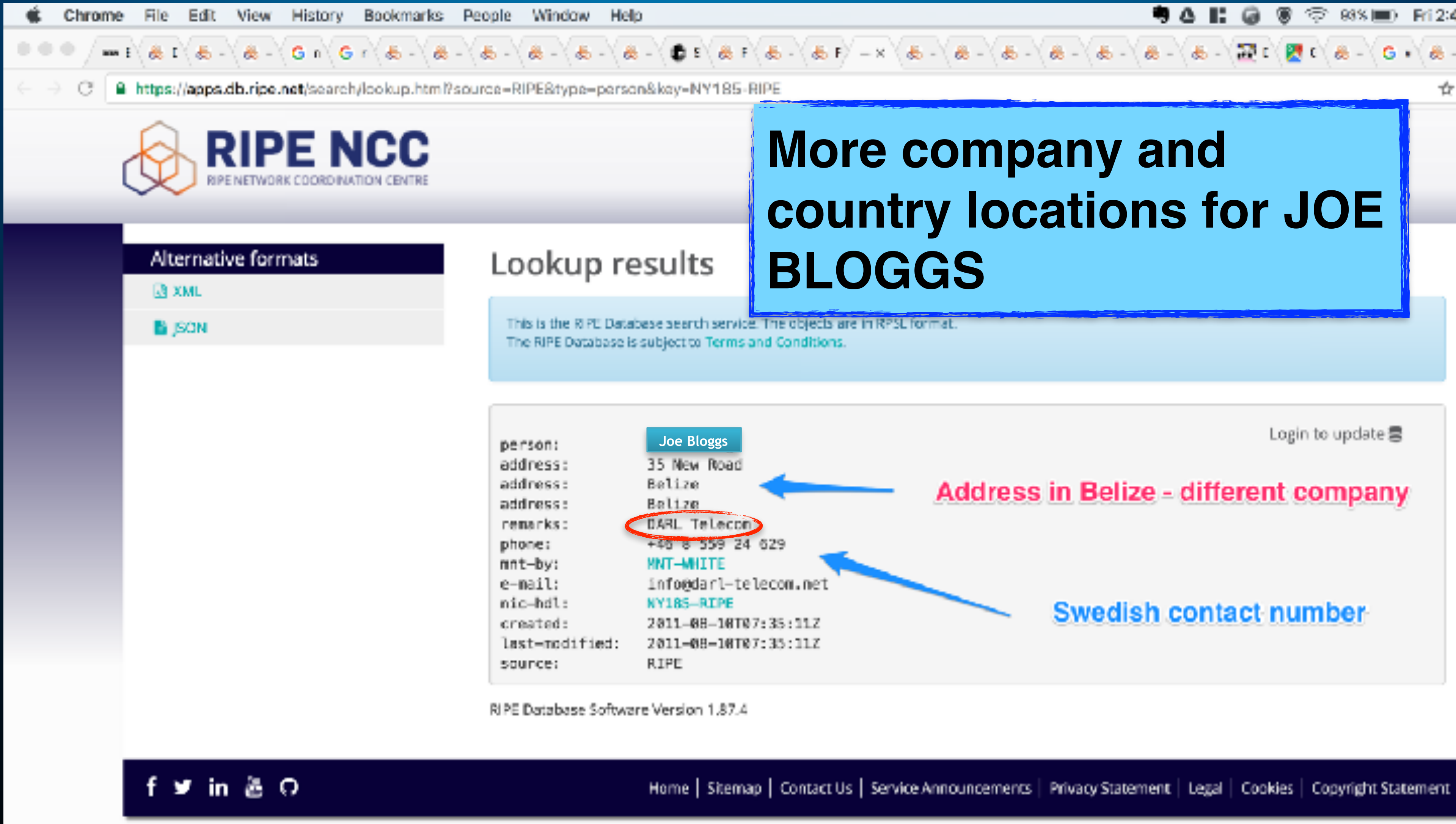
☑ Highlight RIPE NCC managed val

```
organisation:     ORG-sL320-RIPE
org-name:         3nt solutions LLP
org-type:         LIR
address:          3NT SOLUTIONS LLP
address:          Joe Bloggs
address:          10 GREAT RUSSELL STREET SUITE 4004
address:          WC1B 3BQ
address:          LONDON
address:          UNITED KINGDOM
phone:            +442081333030
fax-no:           +441317778303
e-mail:           info@3nt.com
mnt-ref:          RIPE-NCC-HM-MNT
mnt-ref:          MNT-3NT
mnt-by:           RIPE-NCC-HM-MNT
admin-c:          TNTS-RIPE
abuse-c:          ATNT-RIPE
tech-c:           TNTS-RIPE
created:          2011-08-31T13:15:32Z
last-modified:    2015-03-05T12:24:08Z
source:           RIPE
```

RIPE Database Software Version 1.82.4

New company name and address

More company and country locations for JOE BLOGGS



Chrome File Edit View History Bookmarks People Window Help
https://apps.db.ripe.net/search/lookup.html?source=RIPE&type=person&key=NY185-RIPE
RIPE NCC
RIPE NETWORK COORDINATION CENTRE
Alternative formats
XML
JSON
Login to update
Home | Sitemap | Contact Us | Service Announcements | Privacy Statement | Legal | Cookies | Copyright Statement

Lookup results

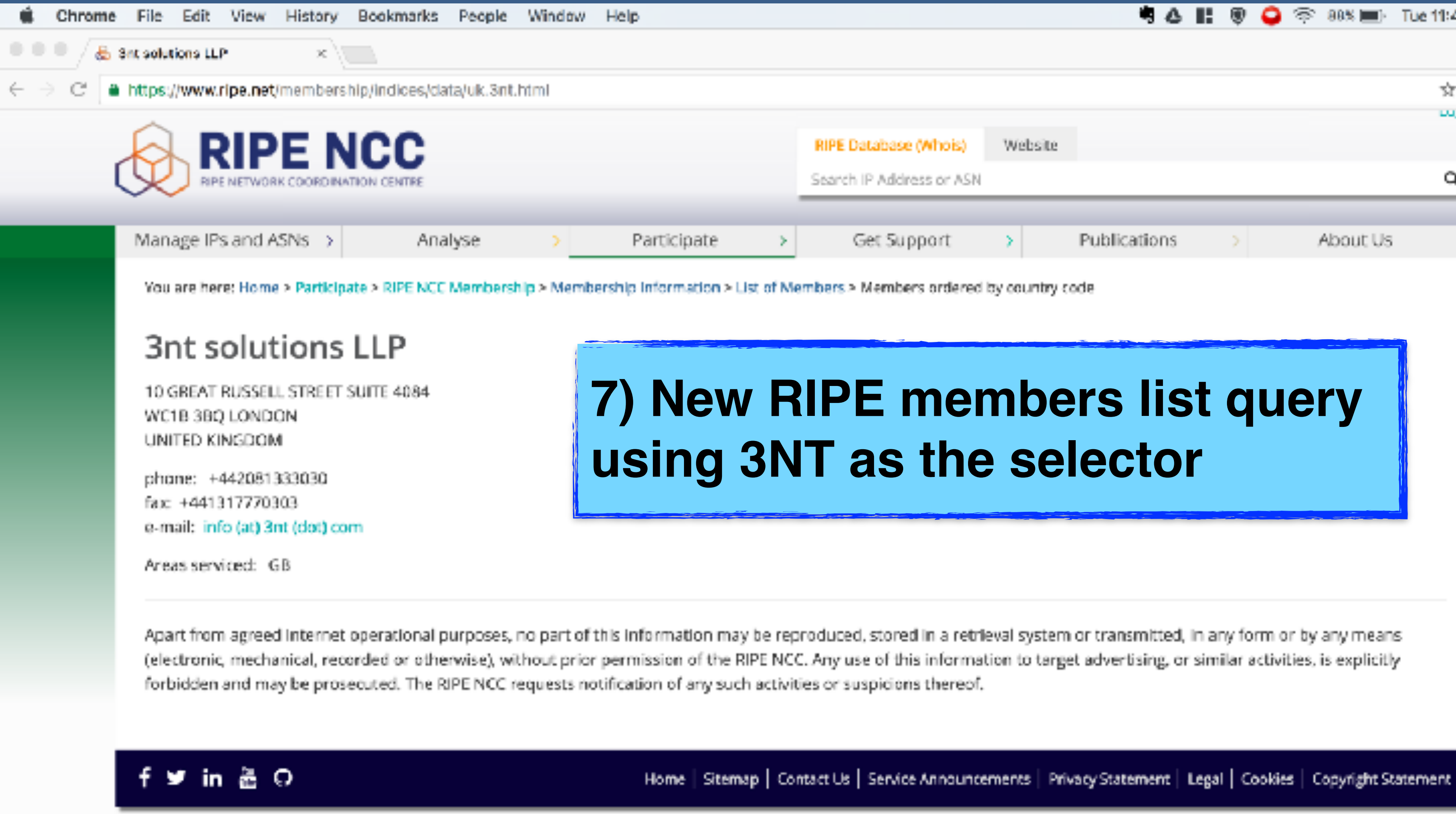
This is the RIPE Database search service. The objects are in RPSL format.
The RIPE Database is subject to Terms and Conditions.

```
person:          Joe Bloggs
address:         35 New Road
address:         Belize
address:         Belize
remarks:         DARL Telecom
phone:           +46 8 559 24 629
mnt-by:          MNT-WHITE
e-mail:          info@darl-telecom.net
nic-hdl:         NY185-RIPE
created:         2011-08-10T07:35:11Z
last-modified:   2011-08-10T07:35:11Z
source:          RIPE
```

RIPE Database Software Version 1.87.4

Address in Belize - different company

Swedish contact number


Chrome File Edit View History Bookmarks People Window Help
3nt solutions LLP
https://www.ripe.net/membership/indices/data/uk.3nt.html
RIPE NCC
RIPE NETWORK COORDINATION CENTRE
RIPE Database (Whois)
Website
Search IP Address or ASN
Manage IPs and ASNs
Analyse
Participate
Get Support
Publications
About Us
Home | Sitemap | Contact Us | Service Announcements | Privacy Statement | Legal | Cookies | Copyright Statement

You are here: Home > Participate > RIPE NCC Membership > Membership Information > List of Members > Members ordered by country code

3nt solutions LLP

10 GREAT RUSSELL STREET SUITE 4084
WC1B 3BQ LONDON
UNITED KINGDOM

phone: +442081333030
fax: +441317770303
e-mail: info (at) 3nt (dot) com

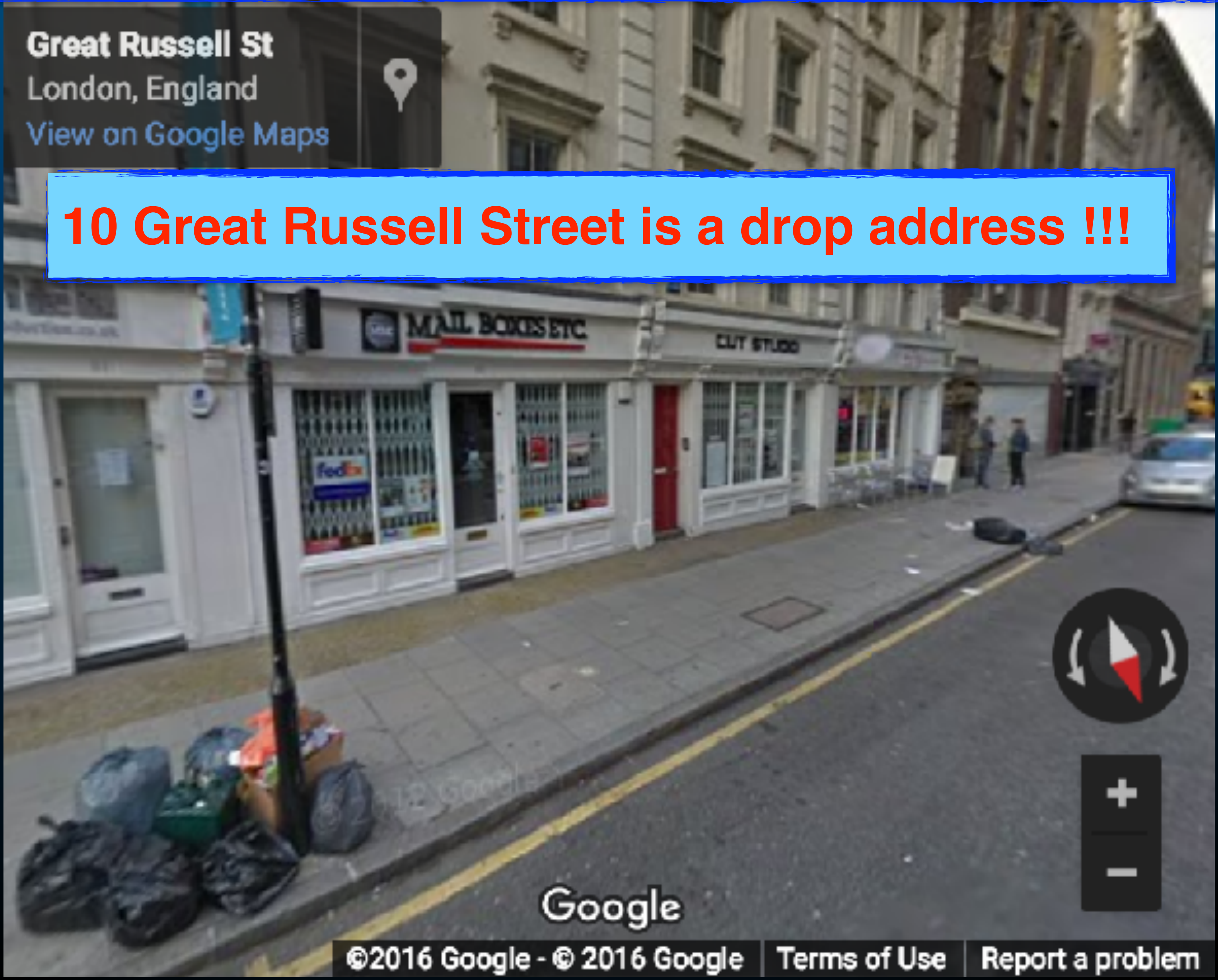
Areas serviced: GB

Apart from agreed Internet operational purposes, no part of this information may be reproduced, stored in a retrieval system or transmitted, in any form or by any means (electronic, mechanical, recorded or otherwise), without prior permission of the RIPE NCC. Any use of this information to target advertising, or similar activities, is explicitly forbidden and may be prosecuted. The RIPE NCC requests notification of any such activities or suspicions thereof.

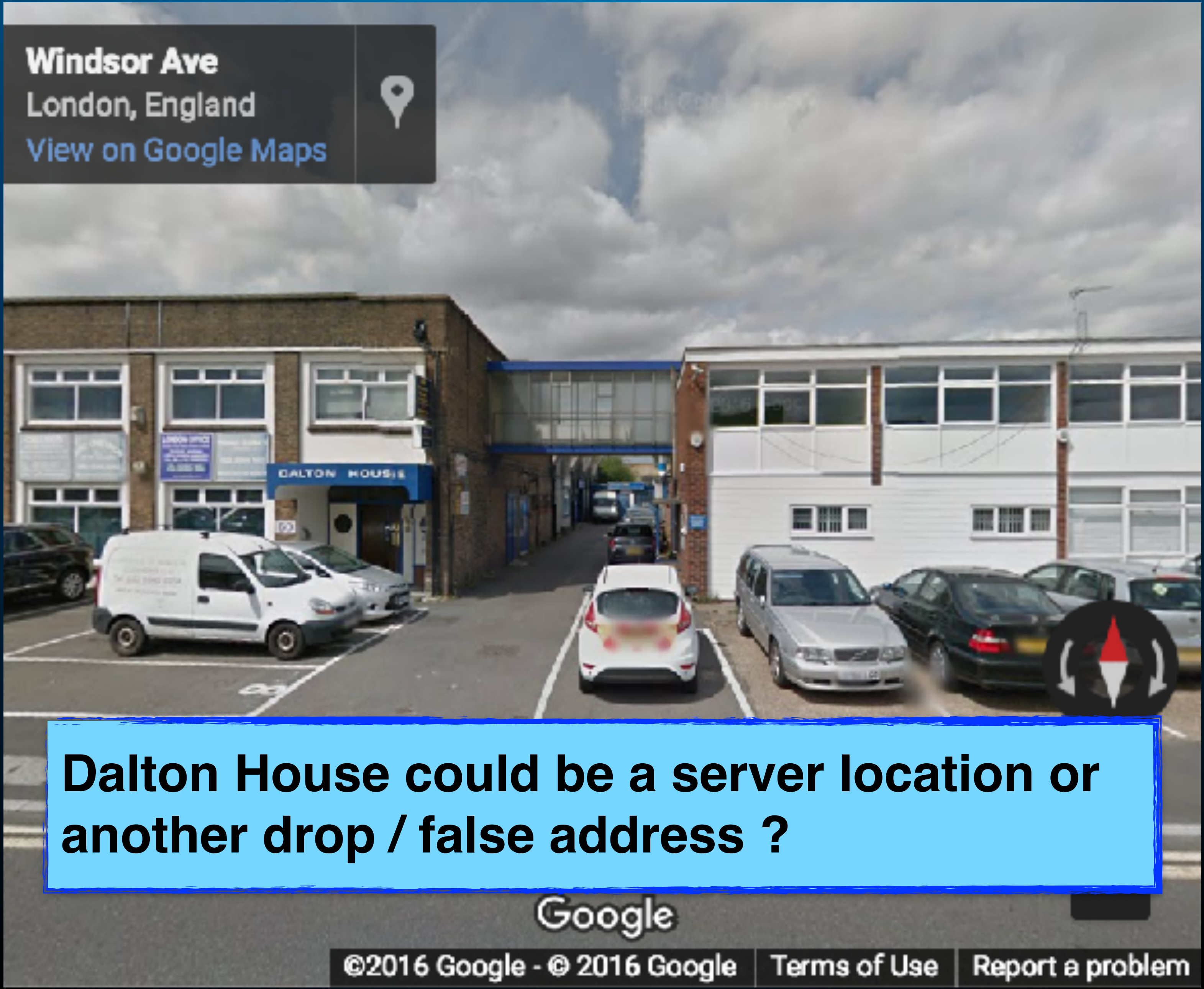
7) New RIPE members list query using 3NT as the selector

Corporate UK name and address now identified ?

8) Query Google Maps against Inferno / 3NT UK registered addresses



10 Great Russell Street is a drop address !!!



Windsor Ave
London, England
View on Google Maps

©2016 Google - © 2016 Google | Terms of Use | Report a problem

Dalton House could be a server location or another drop / false address ?

LLP DESIGNATED MEMBER:
DARL IMPEX LTD
Appointed:
01/04/2011
Nationality:
NATIONALITY UNKNOWN
No. of Appointments: 1
Address: 35 NEW ROAD
BELIZE
NA

9) Query UK Companies House Information for JOE BLOGGS to reveal Darl Telecom and find more company identities

LLP DESIGNATED MEMBER:
LEGRANT TRADING LTD.
Appointed:
19/03/2013
Nationality:
NATIONALITY UNKNOWN
No. of Appointments: 1
Address:
BLAKE BUILDING SUITE 102, GROUND FLOOR, BLAKE BUILDING, CORNER EYRE&HUTSON STREETS
BELIZE CITY
BELIZE
NA

….British Virgin Islands and Panama are also found in more Companies House Records attributed to JOE BLOGGS

(sobbing hysterically)

Inferno Summary

- Still not 100% sure where or who to serve legal process on or the real provider name
- The common UK address for Inferno / 3NT is a suspected drop address (10 Great Russel St.)
- Multiple RIPE member records and handles act as good intelligence to give LE a lead, but…
- Accuracy of records is questionable and is seen across different open source entries
- RIPE member list records and RIPE IP object records are hard to link together
- Multiple company address and country registrations point to 3 different continents

CONCLUSION

- We want to work with the RIPE Community and network operators to develop a policy that would address some of these concerns.
- Mutual interest to act.
- Suggestion:

➡Require <u>registration of all IP sub-allocations to downstream provider</u> so entire chain of sub-allocations are accurately reflected in WHOIS.

(GRUNTING)

Thank you

gregory.mounier@europol.europa.eu