PassiveDNS

UKNOF 20, Bristol, England

9 Sep 2011

Cathy Almond
Internet Systems Consortium

Deck Version 0.2

The global leader in open source DNS

isc.org
Internet Systems Consortium

We make the Internet work better.

BIND 10

The next big thing in DNS

ISC Professional Services

support development
training consulting
audit design

Call in the experts!

SNS@ISC

The ultimate insurance policy for your DNS

ISC is Public Benefit

F-root DHCP
SNS-PB AFTR
BIND and more

Do what you can to support us

RPZ

New method for DNS-based policy enforcement

Taking back the DNS!

SIE

Changing how the security communities productively collaborate

You are here

RPKI

Securing BGP from route hijacking

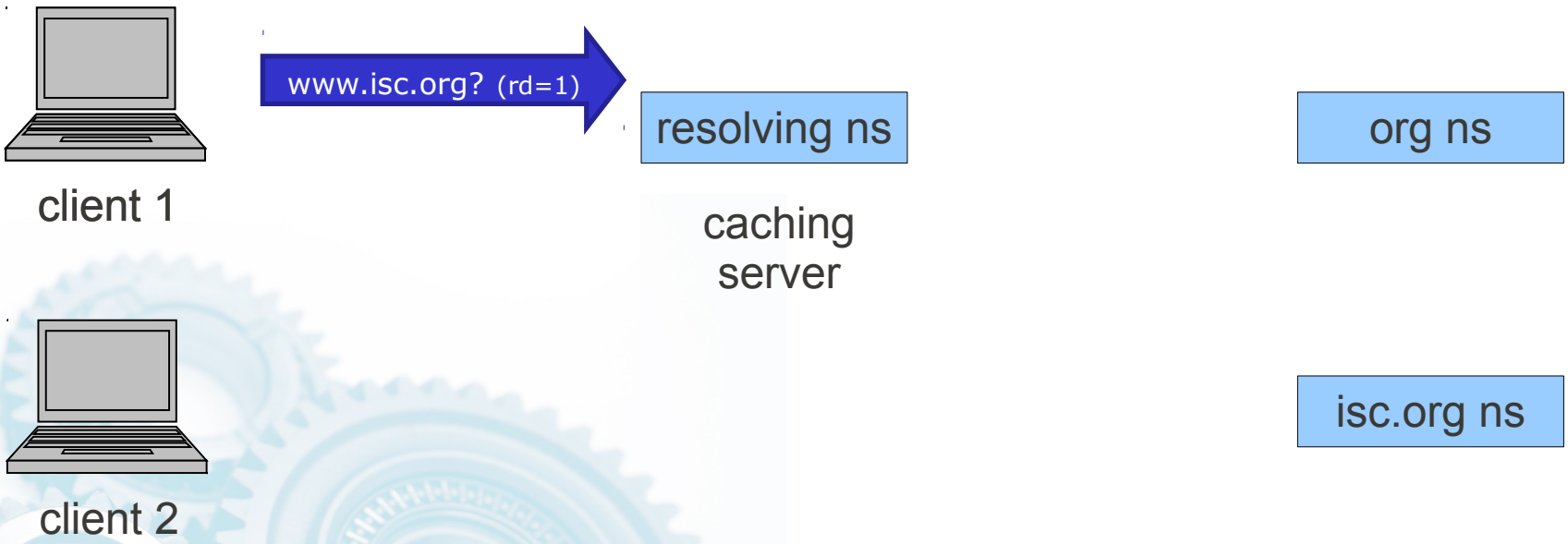
Agenda

- Introduction to PassiveDNS
- How ISC does it
- Examples
- How to participate

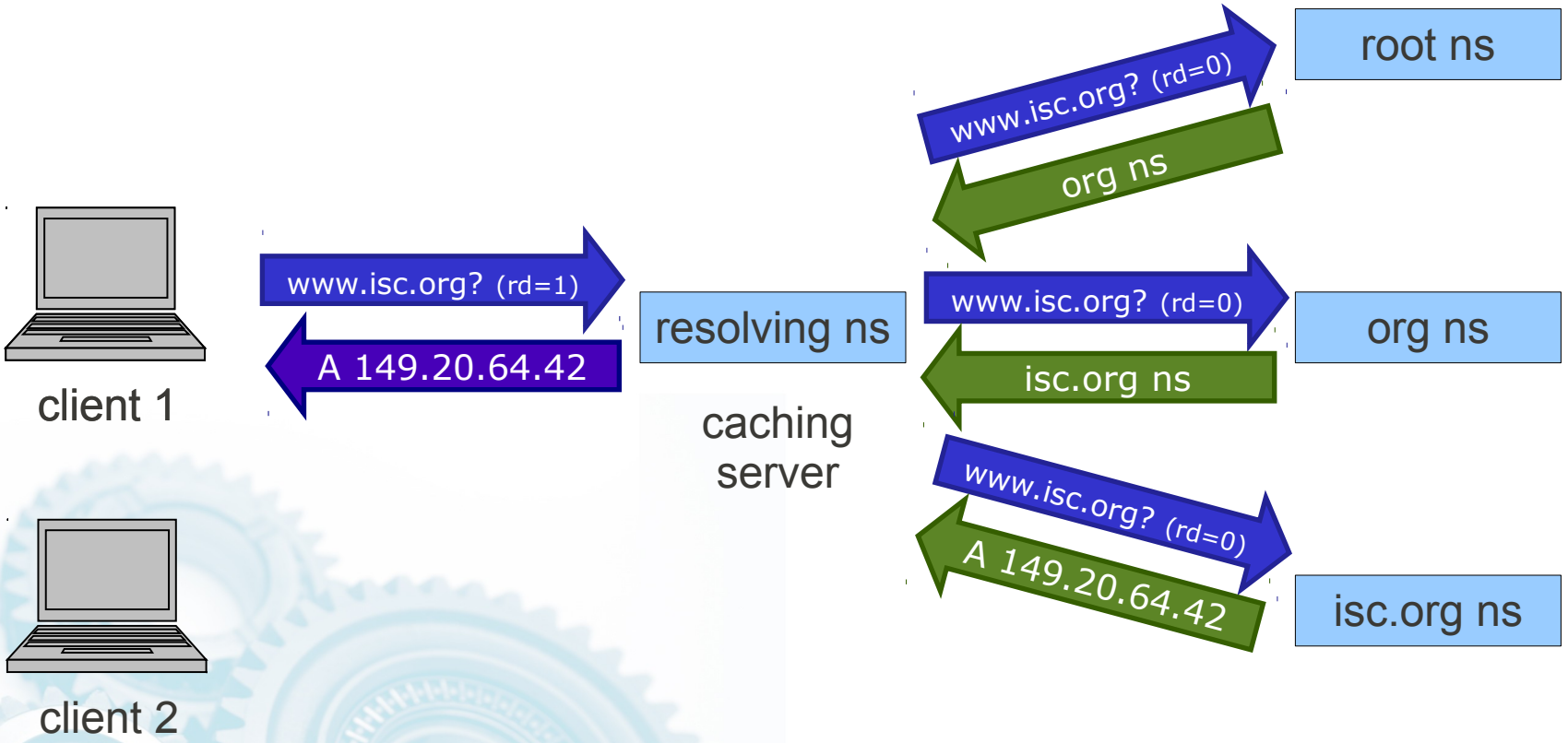
History

- Invented by Florian Weimer in 2004
- Public efforts (RUS-CERT, BFK, DNSparse)
- Use PCAP-based tools (like tcpdump or dnscap) to capture packets, extract data, add to data base, develop query tool
- Used by security community and law enforcement to *passively* analyze associations between badness and the DNS or address resources they use.

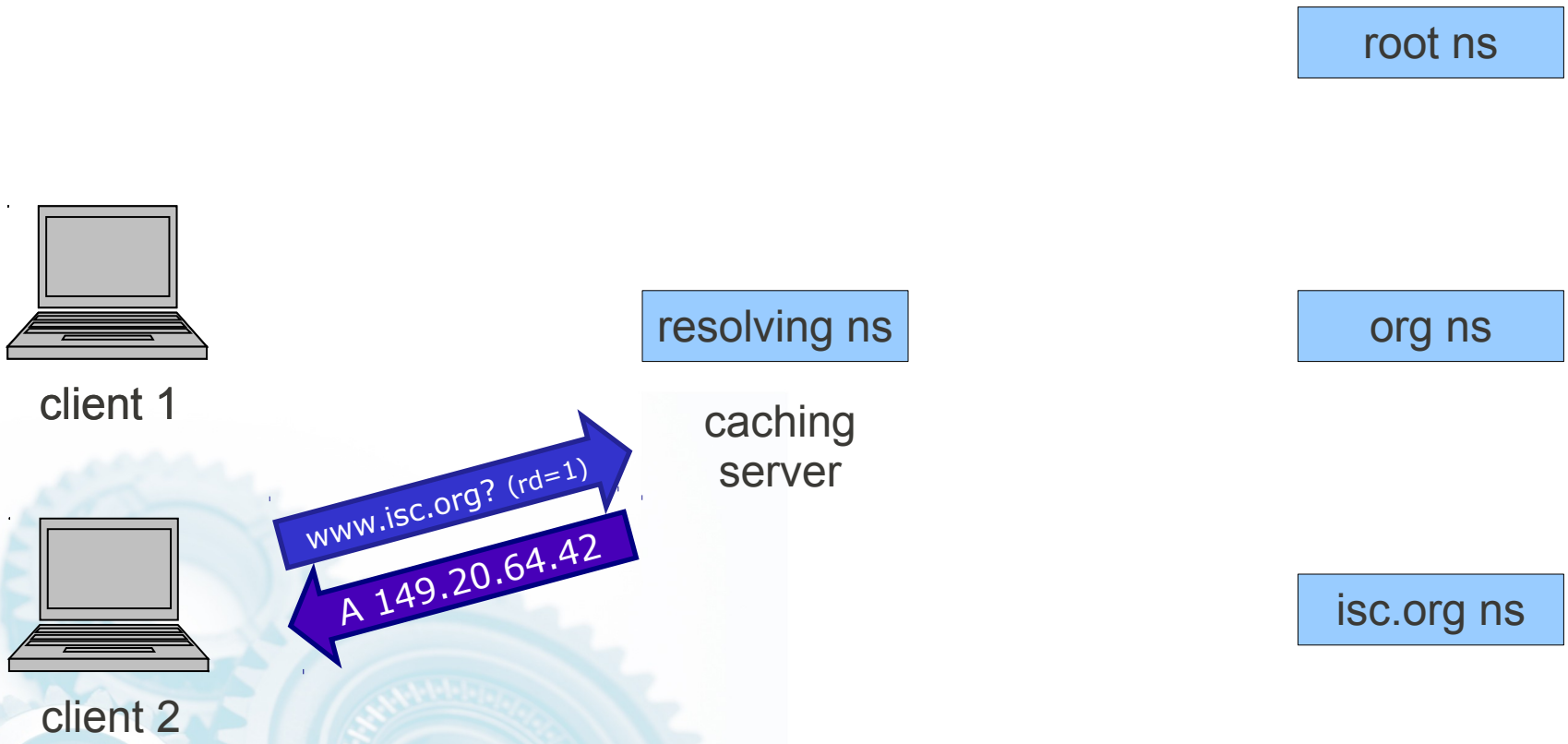
How it works (1st client)



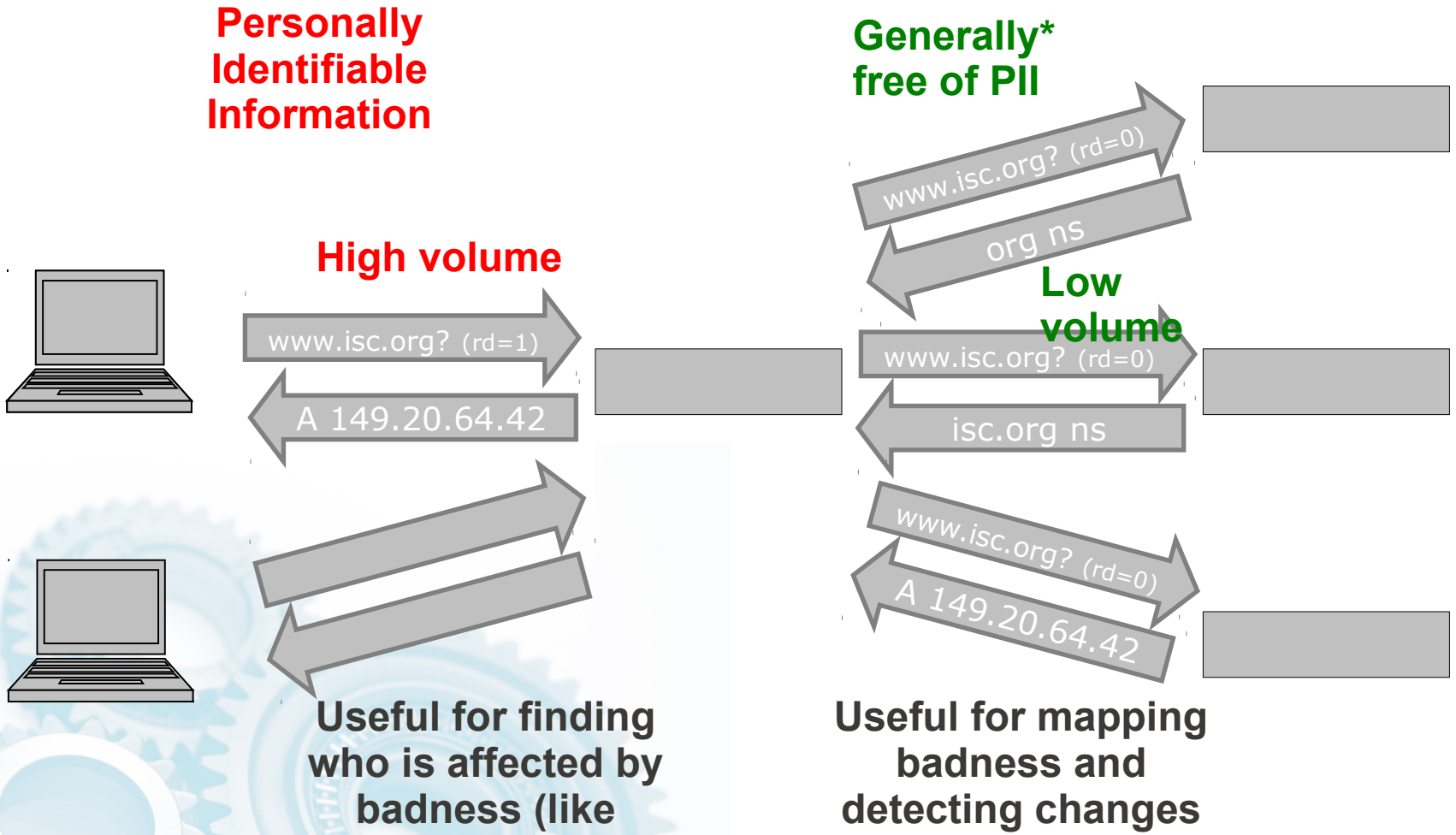
How it works (query/response)



How it works (2nd client)



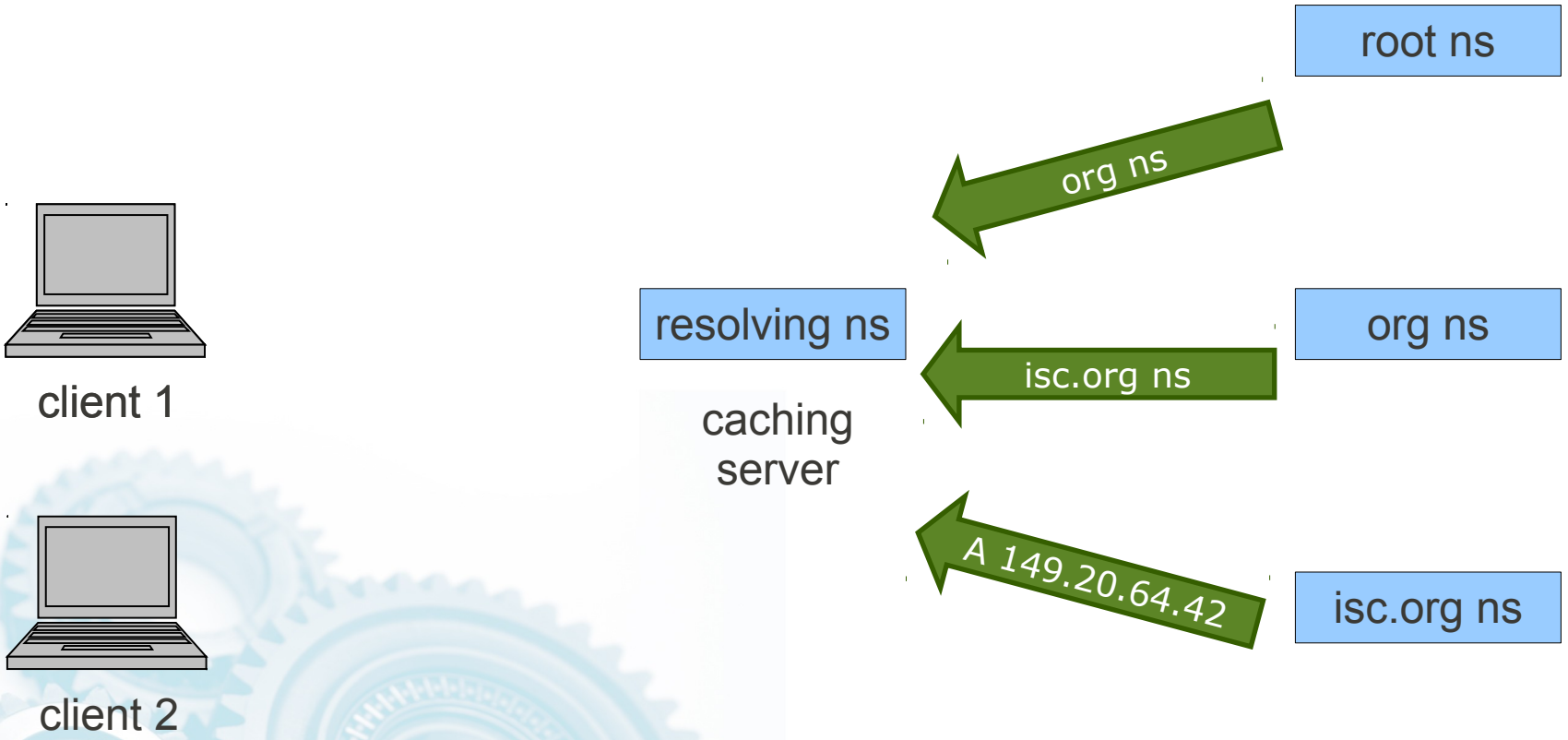
Collection properties



ISC / SIE / DNSDB

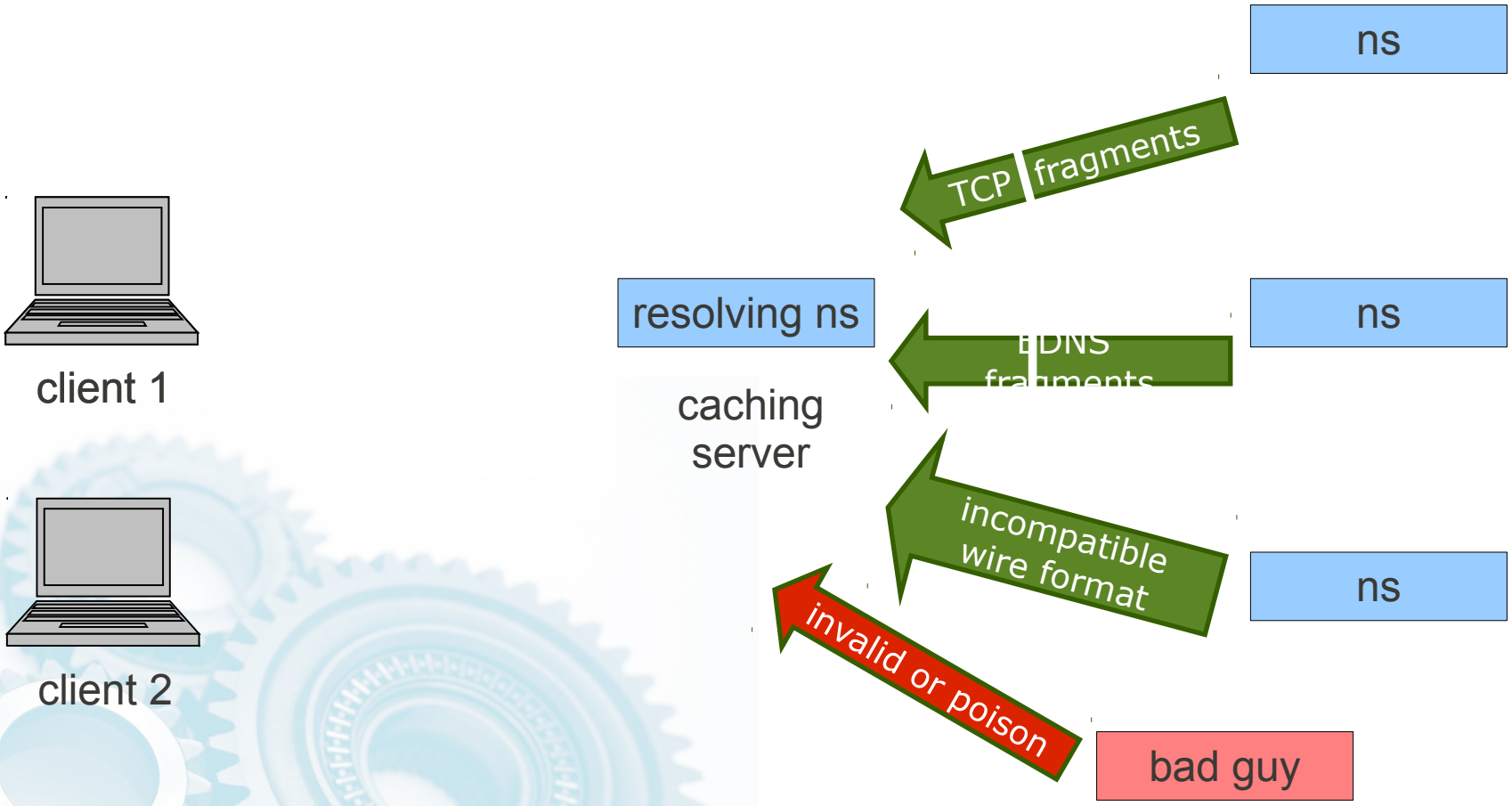
- ISC started in 2007
- Emphasis on high volume collection and near-real-time analysis
- Saw challenges in existing tools
  - Tool evolution
    - dnscap -> ncaptool -> nmsgtool
  - Scalable replication and processing
  - Data storage and access technologies

We like responses

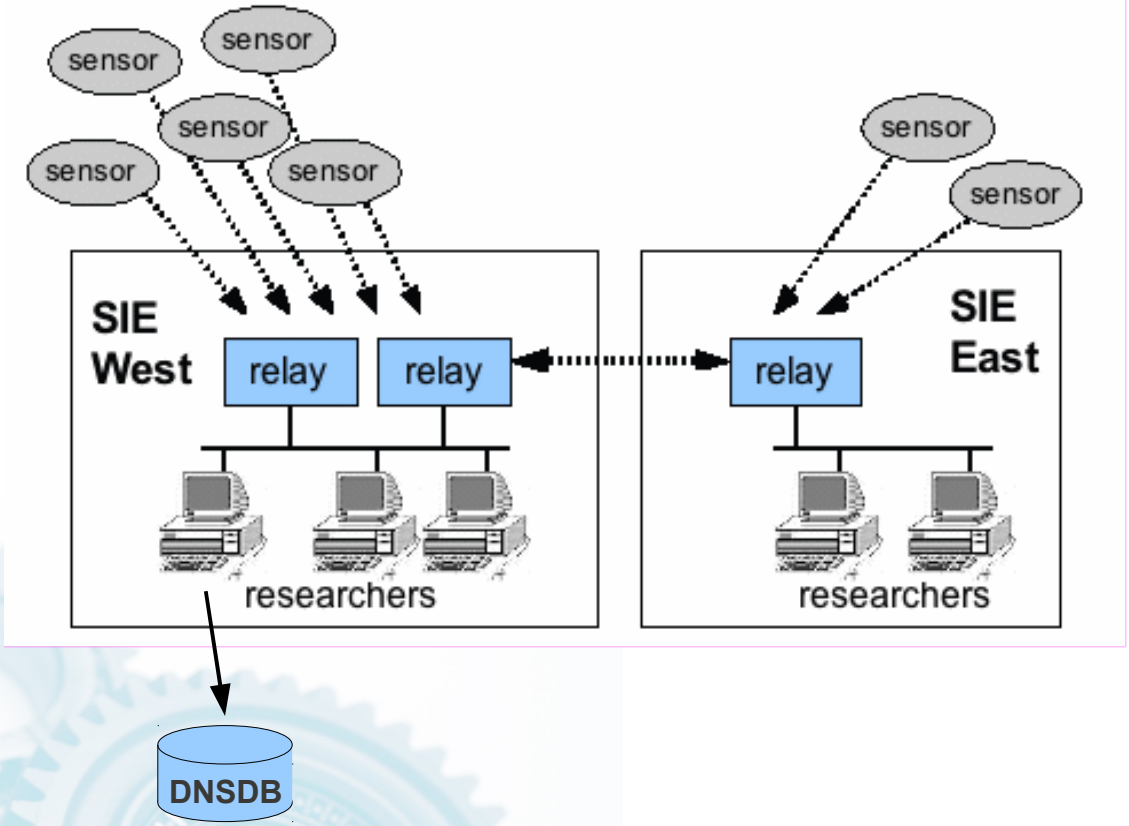


... but that's not good enough.

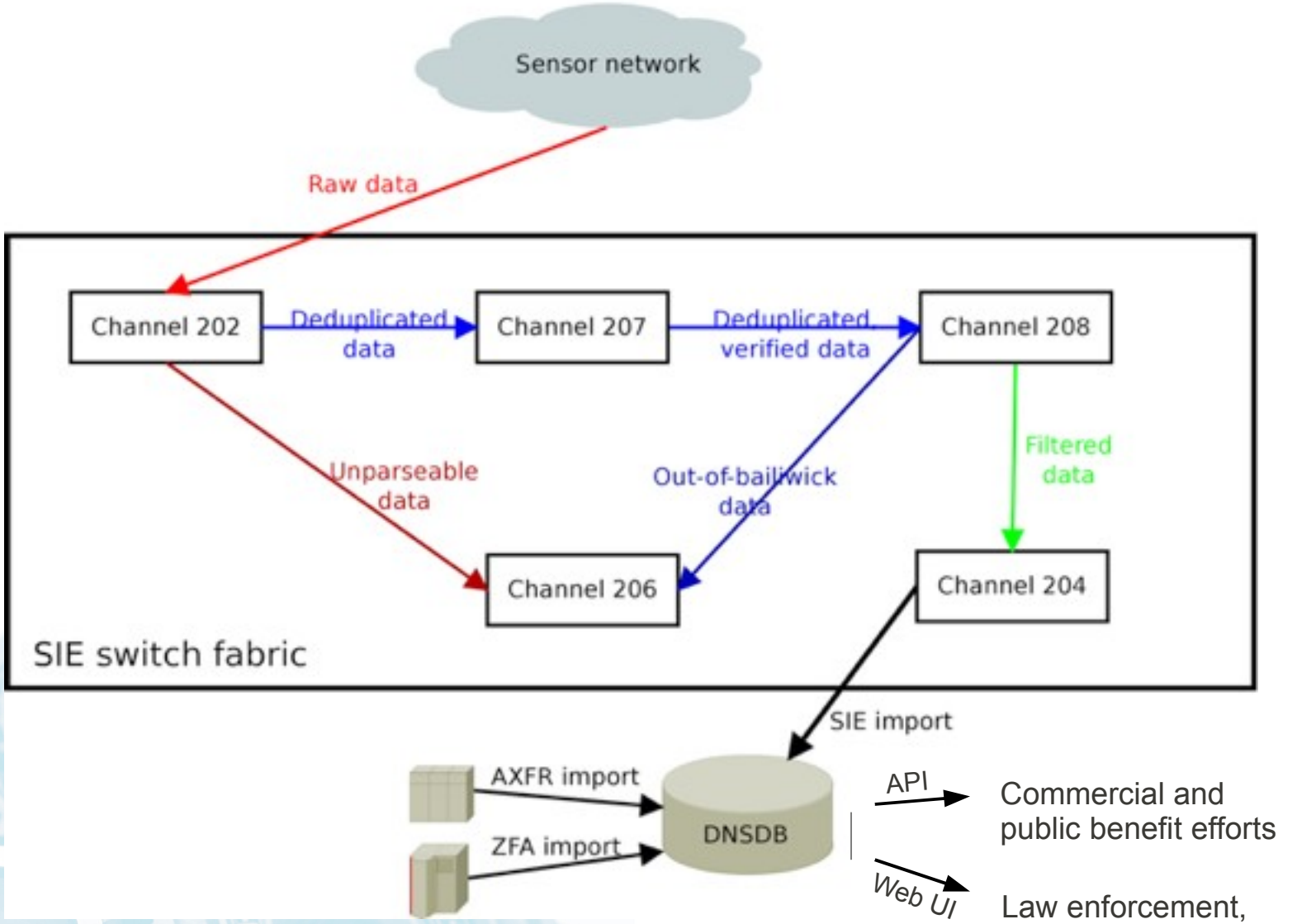
Problems


client 1
client 2
resolving ns
caching server
ns
TCP fragments
EDNS fragments
ns
incompatible wire format
ns
invalid or poison
bad guy

We built some infrastructure (SIE, DNSDB)



ISC Passive DNS and DNSDB architecture



More background

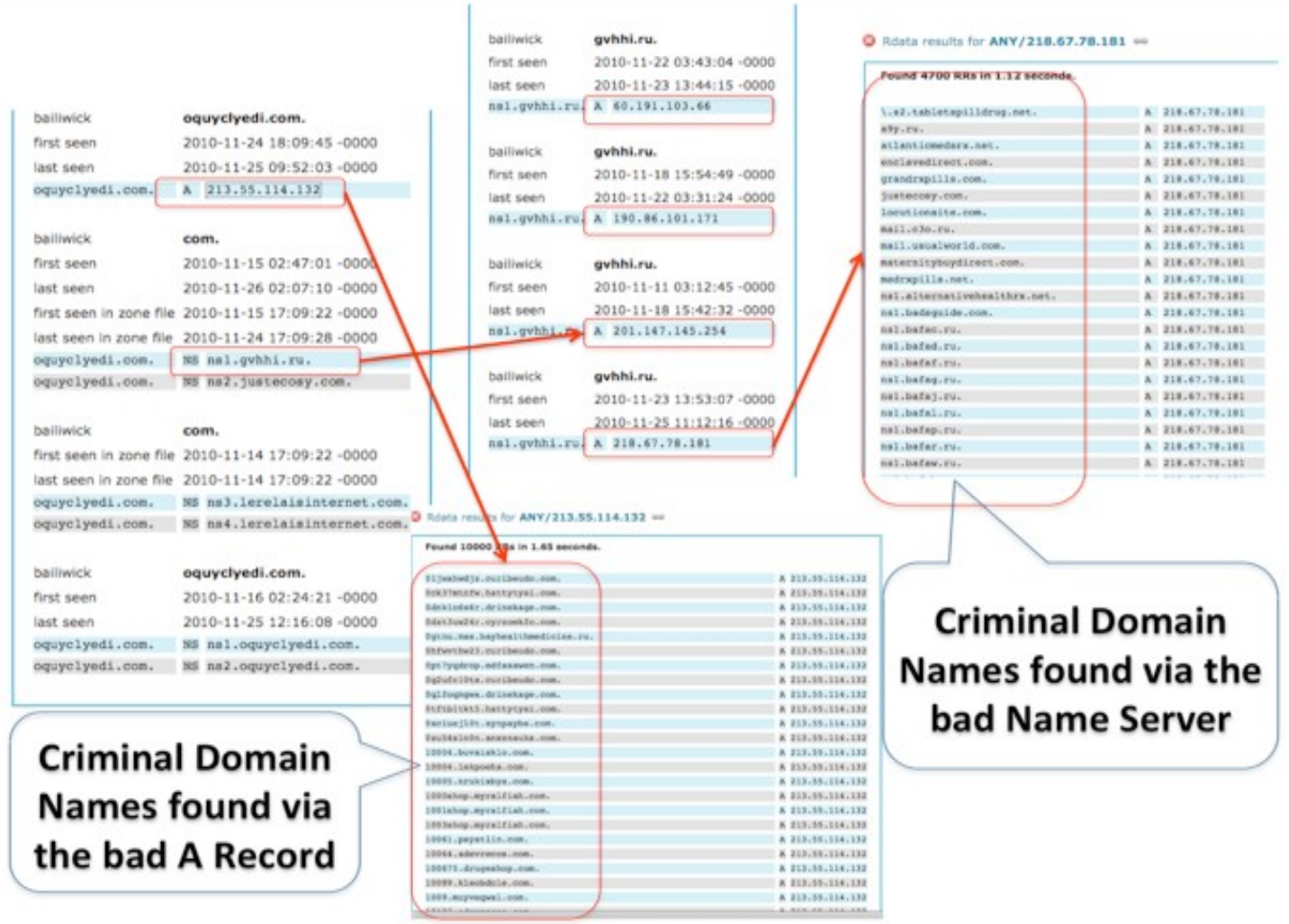
- Robert Edmonds, "Passive DNS Hardening"
  - Video: http://bitly.com/lAJHVZ (DEFCON 18, Jul 2010)
  - Slides: http://www.isc.org/files/passive_dns_hardening_handout.pdf

- ISC Webinar, "SIE & Passive DNS"
  - Video: http://bit.ly/ilpr7k (WebEx, Mar 2011)
  - Slides: https://www.isc.org/files/SIE&Passive%20DNS-2011-03-29_0.pdf
  - Note: Shows examples of how PassiveDNS data has been provided to and used by several research efforts.

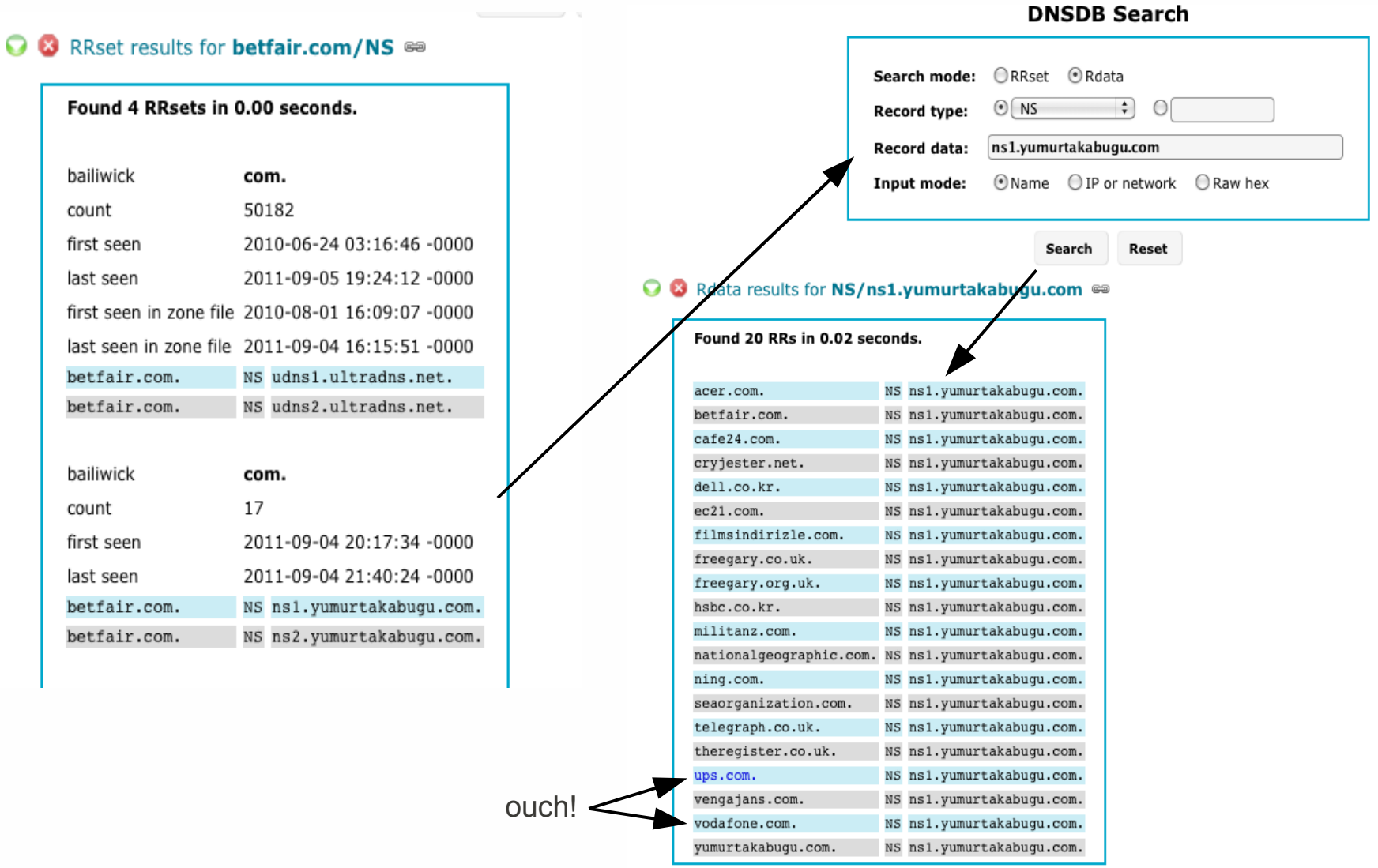
Now some fun


ISC Main
DLV@ISC
SIE@ISC
SNS@ISC
Internet Systems Consortium
Home
Login
DNSDB Login
Username:
Password:
Login
© 2010-2011 Internet Systems Consortium, Inc.
Contact us by sending email to dnsdb@isc.org.

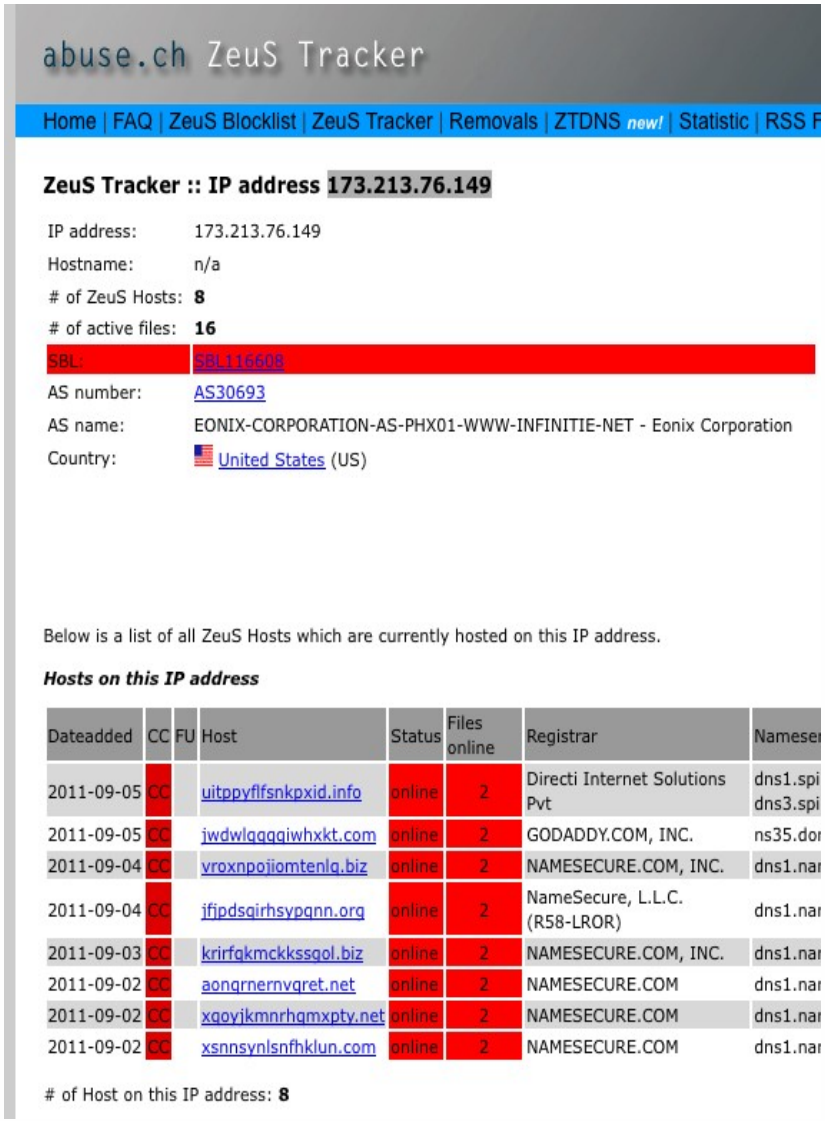
Guilt by association



“... due to a hack at Betfair's registrar”



Zeus hunting (domains)



abuse.ch ZeuS Tracker

Home | FAQ | ZeuS Blocklist | ZeuS Tracker | Removals | ZTDNS *new!* | Statistic | RSS F

ZeuS Tracker :: IP address 173.213.76.149

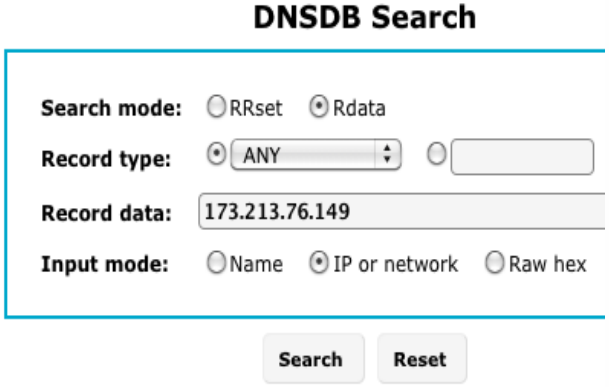
IP address:	173.213.76.149
Hostname:	n/a
# of ZeuS Hosts:	**8**
# of active files:	**16**
SBL:	SBL116608
AS number:	AS30693
AS name:	EONIX-CORPORATION-AS-PHX01-WWW-INFINITIE-NET - Eonix Corporation
Country:	United States (US)

Below is a list of all ZeuS Hosts which are currently hosted on this IP address.

Hosts on this IP address

Dateadded	CC	FU	Host	Status	Files online	Registrar	Nameser
2011-09-05	CC		uitppyflfsnkpxid.info	online	2	Directi Internet Solutions Pvt	dns1.spi dns3.spi
2011-09-05	CC		jwdwlqqqqiwhxkt.com	online	2	GODADDY.COM, INC.	ns35.dor
2011-09-04	CC		vroxnpojiomtenlq.biz	online	2	NAMESECURE.COM, INC.	dns1.nar
2011-09-04	CC		jfjpdsqirhsypqnn.org	online	2	NameSecure, L.L.C. (R58-LROR)	dns1.nar
2011-09-03	CC		krirfqkmckkssgol.biz	online	2	NAMESECURE.COM, INC.	dns1.nar
2011-09-02	CC		aongrnernvqret.net	online	2	NAMESECURE.COM	dns1.nar
2011-09-02	CC		xqoyjkmnrhqmxpty.net	online	2	NAMESECURE.COM	dns1.nar
2011-09-02	CC		xsnnsynlsnfhklun.com	online	2	NAMESECURE.COM	dns1.nar

# of Host on this IP address: **8**



DNSDB Search

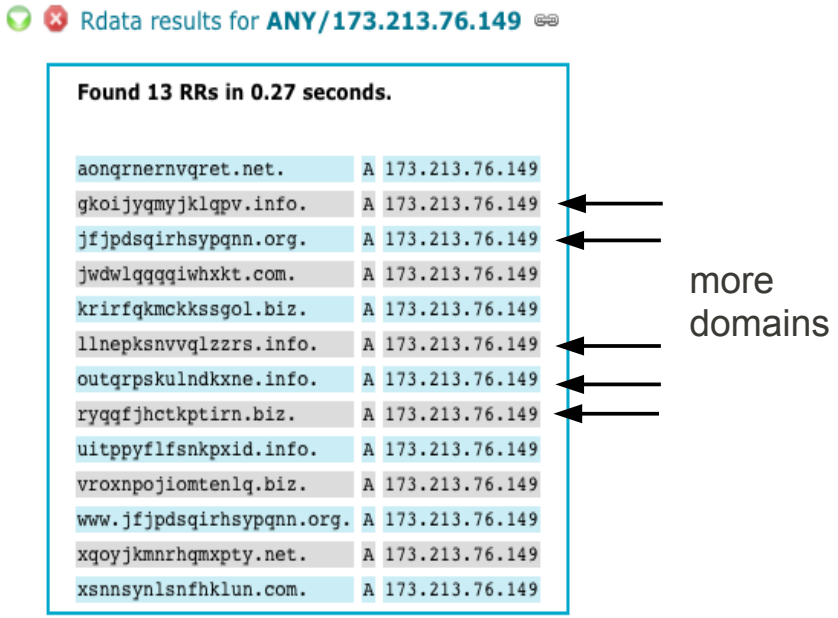
Search mode: RRset Rdata

Record type: ANY

Record data: 173.213.76.149

Input mode: Name IP or network Raw hex

Search **Reset**



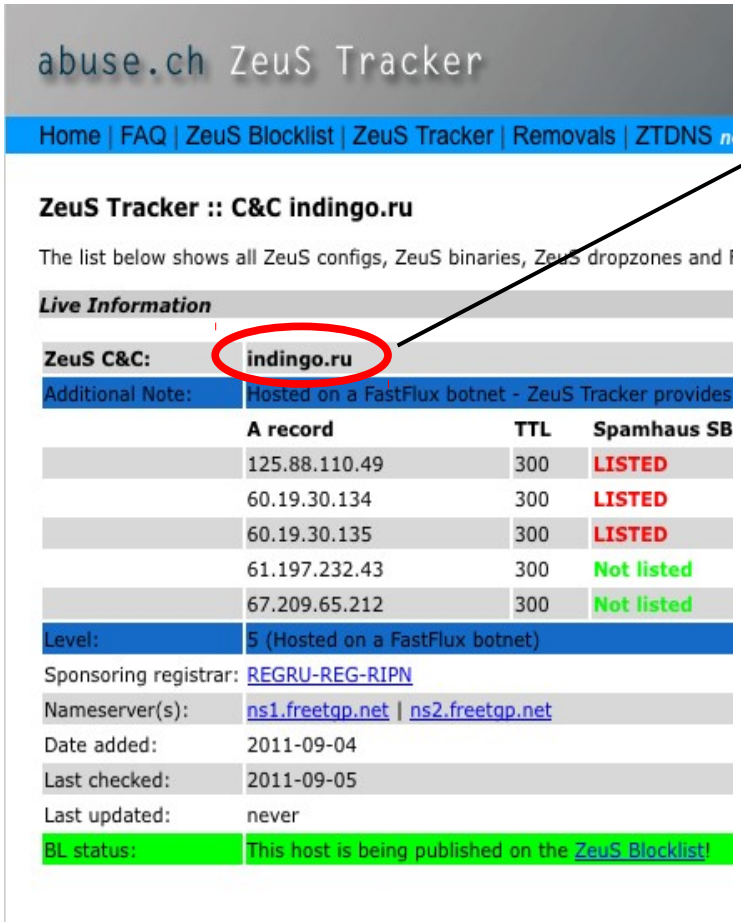
Rdata results for **ANY/173.213.76.149**

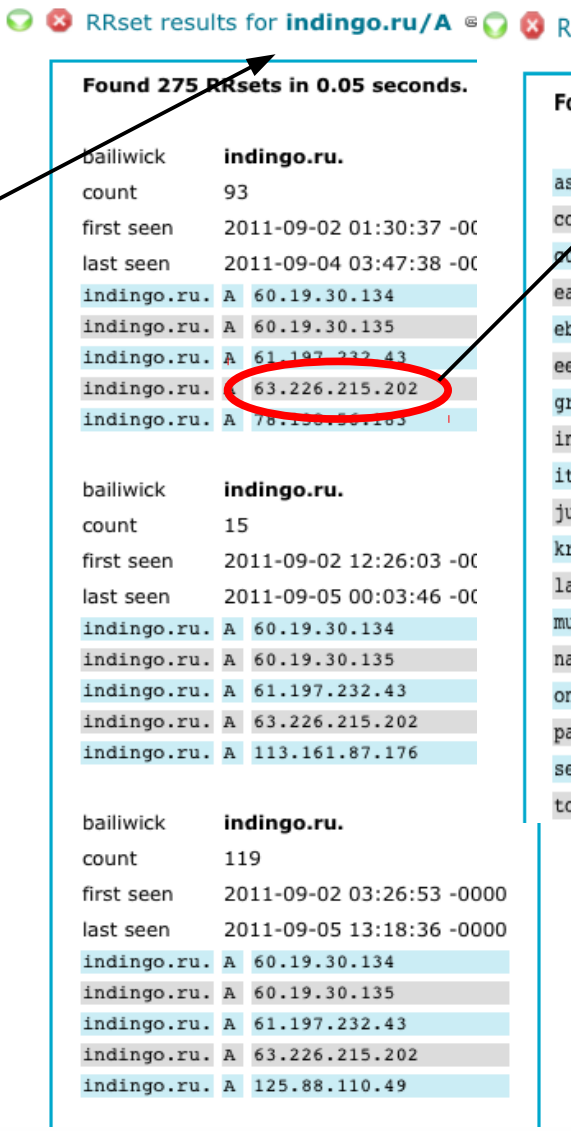
Found 13 RRs in 0.27 seconds.

aongrnernvqret.net.	A	173.213.76.149
gkoijyqmyjklqpv.info.	A	173.213.76.149
jfjpdsqirhsypqnn.org.	A	173.213.76.149
jwdwlqqqqiwhxkt.com.	A	173.213.76.149
krirfqkmckkssgol.biz.	A	173.213.76.149
llnepksnvvqlzzrs.info.	A	173.213.76.149
outqrpskulndkxne.info.	A	173.213.76.149
ryqqfjhctkptirn.biz.	A	173.213.76.149
uitppyflfsnkpxid.info.	A	173.213.76.149
vroxnpojiomtenlq.biz.	A	173.213.76.149
www.jfjpdsqirhsypqnn.org.	A	173.213.76.149
xqoyjkmnrhqmxpty.net.	A	173.213.76.149
xsnnsynlsnfhklun.com.	A	173.213.76.149

more domains

Zeus hunting (fast-flux)





... more domains
... more IP resources

One good spam deserves another...

[162] [2011-09-06 05:31:35.########] [1:2 ISC email]
type: spamtrap
srchost: 117.*yyy.yy.yyy*
bodyurl: hxxp://Despo.pharmacyramat.ru/?*xxxxxxxxxxxxx*
... redirects to "hxxp://www.medicostb.com/"

RRset results for **despo.pharmacyramat.ru/ANY**

Found 1 RRsets in 0.07 seconds.

bailiwick	**pharmacyramat.ru.**
count	33
first seen	2011-09-01 18:24:29 -0000
last seen	2011-09-05 19:06:38 -0000
despo.pharmacyramat.ru.	A 115.239.229.196
despo.pharmacyramat.ru.	A 122.224.18.23

Rdata results for **ANY/115.239.229.196**

Found 10000 RRs in 10.43 seconds.

1137.pfizer.ismedic.ru.	A	115.239.229.196
14dd.pfizer.medicac.ru.	A	115.239.229.196
2867.pfizer.ismedic.ru.	A	115.239.229.196
41.pfizer.medicac.ru.	A	115.239.229.196
4623.pfizer.ismedic.ru.	A	115.239.229.196
a.aawlj.cswfex.pfizer.medicac.ru.	A	115.239.229.196
a.abub37gzyut.pfizer.ismedic.ru.	A	115.239.229.196
a.acehmdd.pfizer.medicac.ru.	A	115.239.229.196
a.acjol4xusw.pfizer.medicac.ru.	A	115.239.229.196
a.acquard.pfizer.medicac.ru.	A	115.239.229.196
a.ad81yahoo.de.pfizer.ismedic.ru.	A	115.239.229.196
a.atte.vinicio12d.pfizer.medicac.ru.	A	115.239.229.196
a.ayoka9.pfizer.ismedic.ru.	A	115.239.229.196
a.bschaper.pfizer.medicac.ru.	A	115.239.229.196
a.cadet001.pfizer.ismedic.ru.	A	115.239.229.196
a.calavera35.pfizer.medicac.ru.	A	115.239.229.196
a.califjoy.pfizer.ismedic.ru.	A	115.239.229.196
a.candy1669.pfizer.ismedic.ru.	A	115.239.229.196

DNSDB API

```
$ DNSDB_FORMAT=json isc-dnsdb-query rdata ip 192.0.32.10 | sort
{"rrtype": "A", "rrname": "example.com.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "example.edu.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "example.net.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "example.org.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "mal1.gbs-clan.de.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "mail2.gbs-clan.de.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "scribble.co.uk.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "www.example.com.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "www.example.edu.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "www.example.net.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "www.example.org.", "rdata": "192.0.32.10"}
```

... for programmed lookups and cross-references and search.
... gets around web browser javascript limitations.

... using API with last example

```
$ dig medicostb.com ns
medicostb.com.          169386  IN    NS  ns1.upsdns.com.ua.
medicostb.com.          169386  IN    NS  ns2.dnsaq.ru.

$ ( for f in `isc_dnsdb_query.py -n ns1.upsdns.com.ua/NS | \
     awk '{print $1}'`; do isc_dnsdb_query.py -r $f -j |\
    egrep 'time_last": 1315[12]'; done) | awk '{print $8}' | sort -u
"healthtr.com.",
"medicacpr.ru.",
"medicannk.com.",
"mediccker.ru.",
"medicckIr.ru.",
"medicehok.com.",
"medicelcr.ru.",
"medicellk.com.",
"medicemur.ru.",
"medicheek.com.",
"medichmar.ru.",
...etc...
```

Other uses

- Look up what names are hosted on your networks (by CIDR).
- Look at what is hosted around CIDR a bulletproof hosting site.
- Look for delisted domains and watch them move around.
- Look at DNSSEC history for domains.
- Look at IPv6 utilization.
- Look at resources hosted by dynamic or low-cost DNS providers (eg: *.cz.cc).
- Rebuild TLD zone files from PassiveDNS data.
- Find new names hosted in ccTLDs (live off the wire).
- Track trademarked names against phishing (live off the wire).

Who gets access?

- Security Information Exchange Peers
- DNSDB User Interface (beta)
  - Vetted member of Operational Security community
  - Passive DNS contributors
  - SIE forum members
  - SIE peers
- DNSDB API (beta)
  - Passive DNS contributors
  - ISC Sponsored Researchers
  - SIE Peers
  - SIE Forum members

How to participate?

- Check out information at https://sie.isc.org
  - Apply to contribute Passive DNS data
  - Download sie-dns-sensor software
  - Gain credentials to allow you to submit PassiveDNS data
  - Configure the sensor software
  - Start feeding data
  - Use benefits of PassiveDNS to help with you own organization's security – get a UI or API account
- E-mail: dnsdb@isc.org