DNS Removals

- Changing a TLD server's address -

Peter Koch <koch@denic.de>

OARC DNS Operational Meeting

Ottawa, 25-SEP-2008

What we did

- Changed address of S.DE.NET
  - 193.159.170.149 -> 195.243.137.26
  - Same AS, no significant RTT change
  - This is a DE only name server
- Captured query traffic
  - Determine dominant source for the address
  - Count queries and queriers
  - Find *Query Swing*
  - Find *Stalking Resolvers*
    - cf. work for B and J root servers

How does DNS traffic go to S.DE.NET?

- Server's name appears
  - in the authoritative NS RRSet at `DE` zone apex
  - in the delegation in the parent zone
- Server's address originates from
  - Authoritative data in `DE.NET`
  - Root zone *glue* data spread through TLD referrals
  - [additional section for authoritative `DE` responses]
  - Surprise, wait …

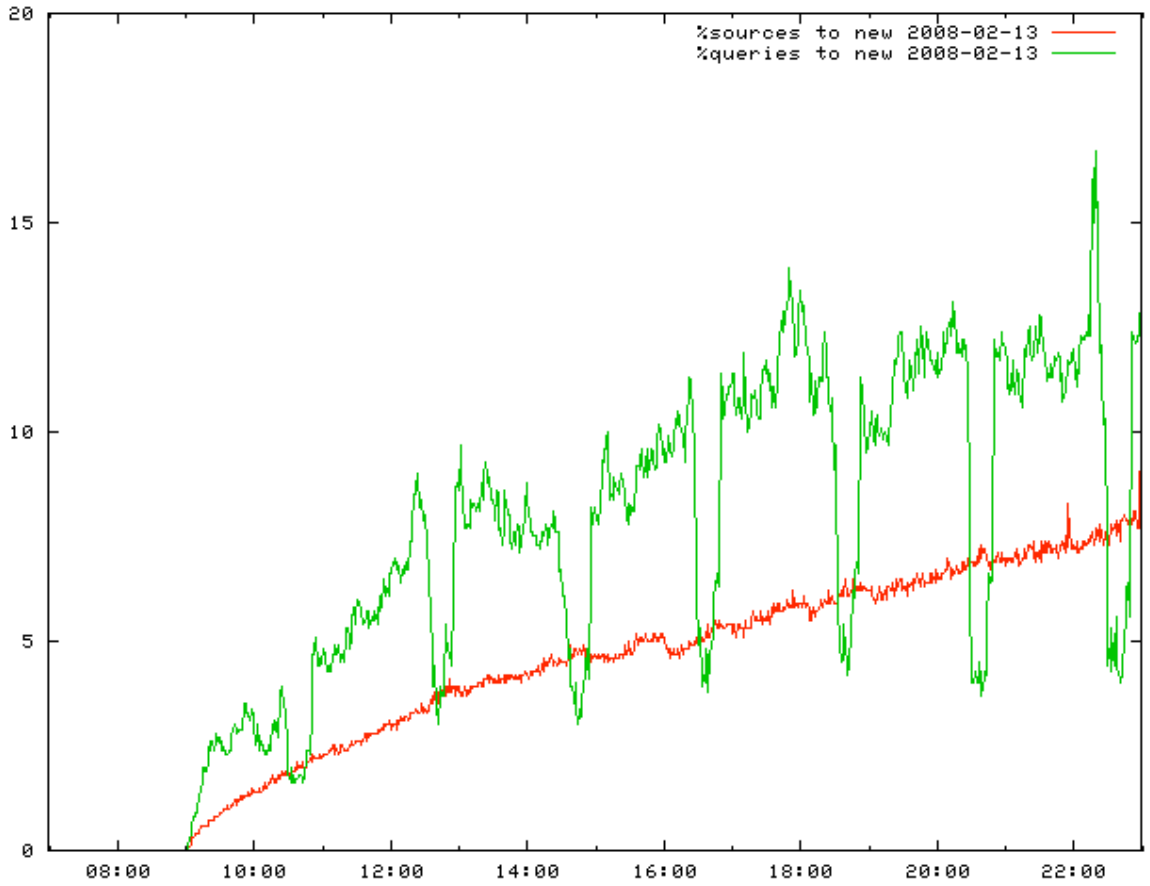
Timeline

- Change of authoritative data in `DE.NET` zone
  - effective 2008-02-13 09:00 2008 UTC
  - TTL was 3600
- Change of „glue“ in the `NET` zone
  - effective 2008-02-20 16:23 2008 UTC
  - TTL was 172800
- Root zone delegation change (glue)
  - effective 2008-02-21 15:37 2008 UTC
  - TTL was 172800

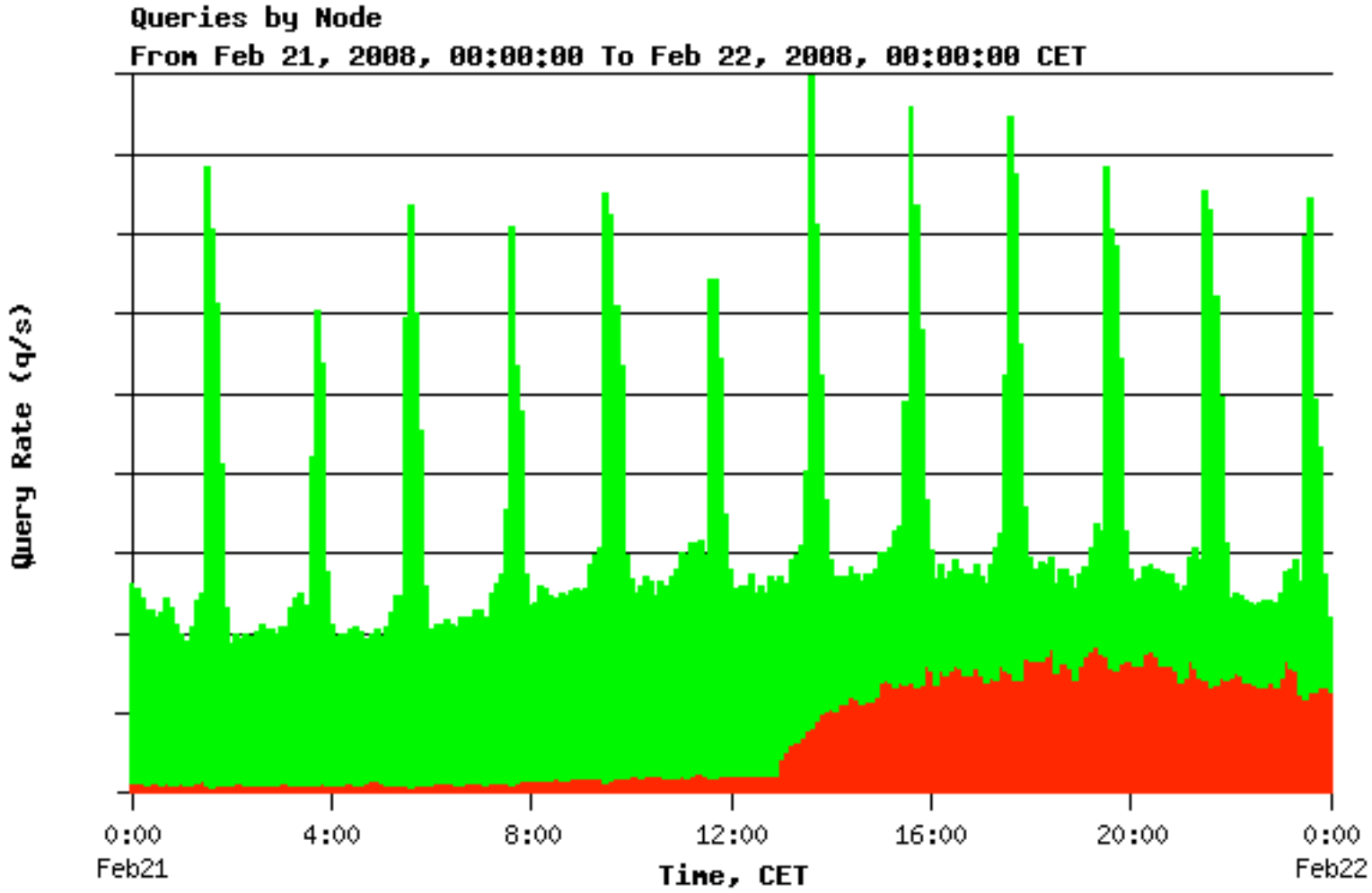
The Unexpected Glue Entry

```
; <<>> DiG 8.4 <<>> +norec @c.gtld-servers.NET. s.de.net.

;; res options: init defnam dnsrch
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43508
;; flags: qr; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 2
;; QUERY SECTION:
;;      s.de.net, type = A, class = IN

;; ANSWER SECTION:
s.de.net.                172800 IN A         195.243.137.26

;; AUTHORITY SECTION:
de.net.                  172800 IN NS        ns1.denic.de.
de.net.                  172800 IN NS        ns2.denic.de.
de.net.                  172800 IN NS        ns3.denic.de.
de.net.                  172800 IN NS        ns4.denic.net.
de.net.                  172800 IN NS        ns5.denic.net.

;; ADDITIONAL SECTION:[…]
```

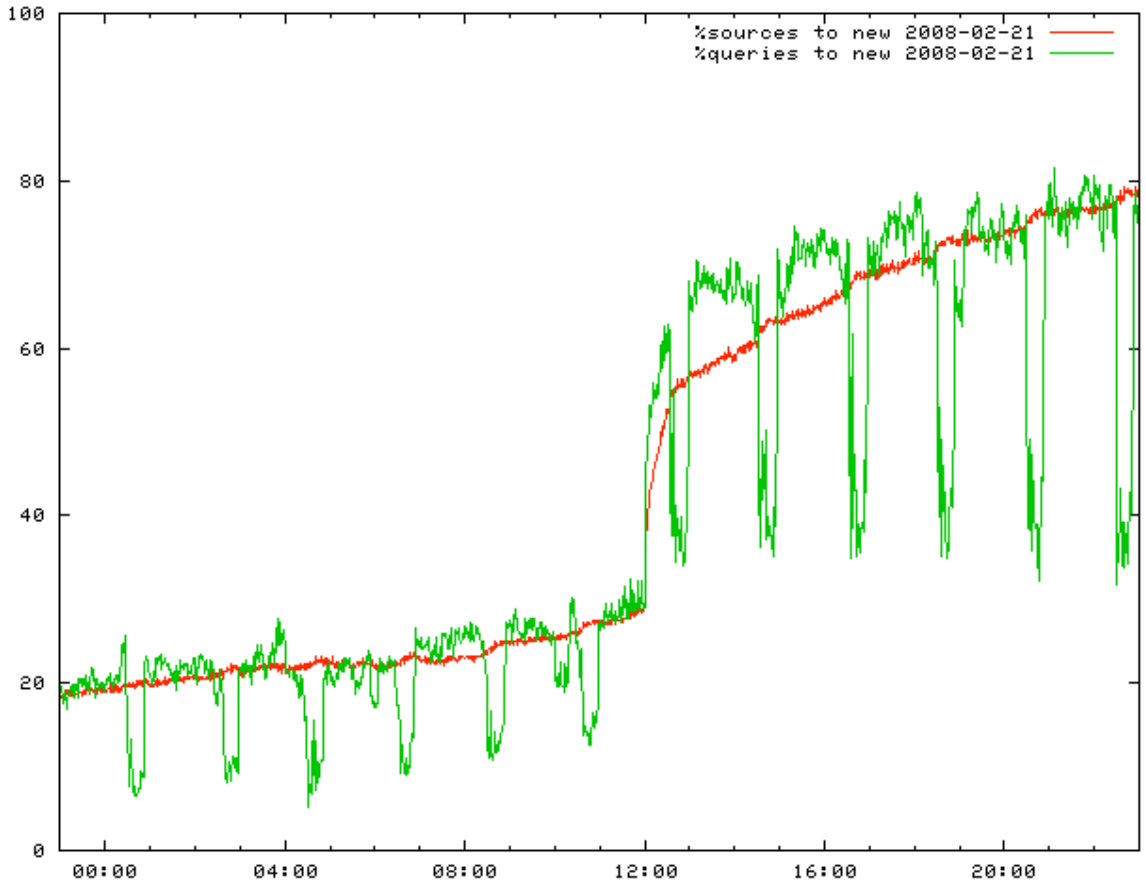
Observations on 2008-02-13 (auth data change)



DSC on 2008-02-21



Stats on 2008-02-21



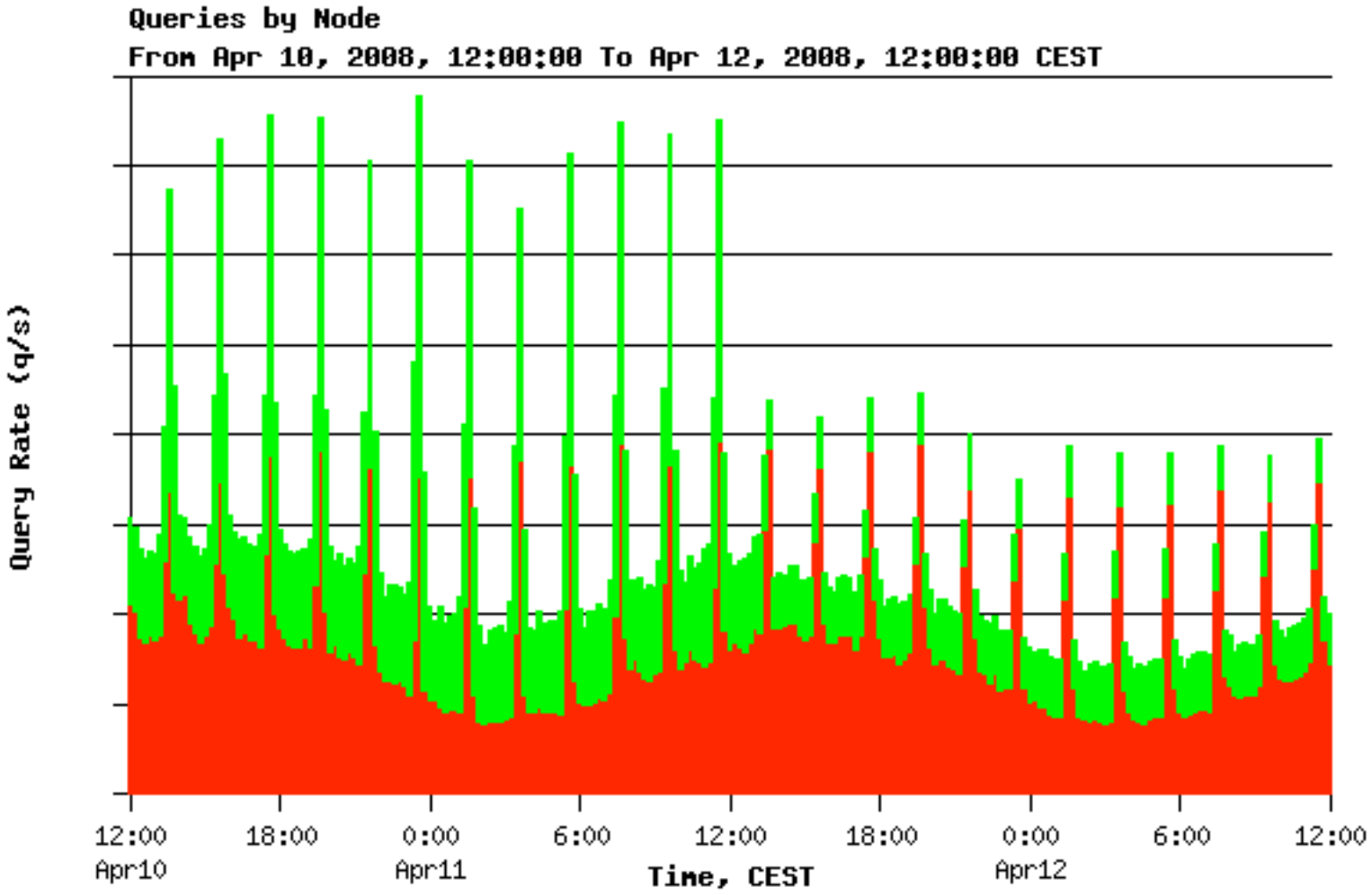
Preliminary Conclusions

- Authoritative data **less** dominant than referral (from root) data
  - Additional section filled from *glue*
- No immediate correlation with root zone dist?
- We have many „first contacts“
- But:
  - This is for an out-of-domain server
  - Special handling of `NET` zone needs to be considered
  - `DE` is largely, but not solely a *delegation only* zone
  - Sensor died due to real world move

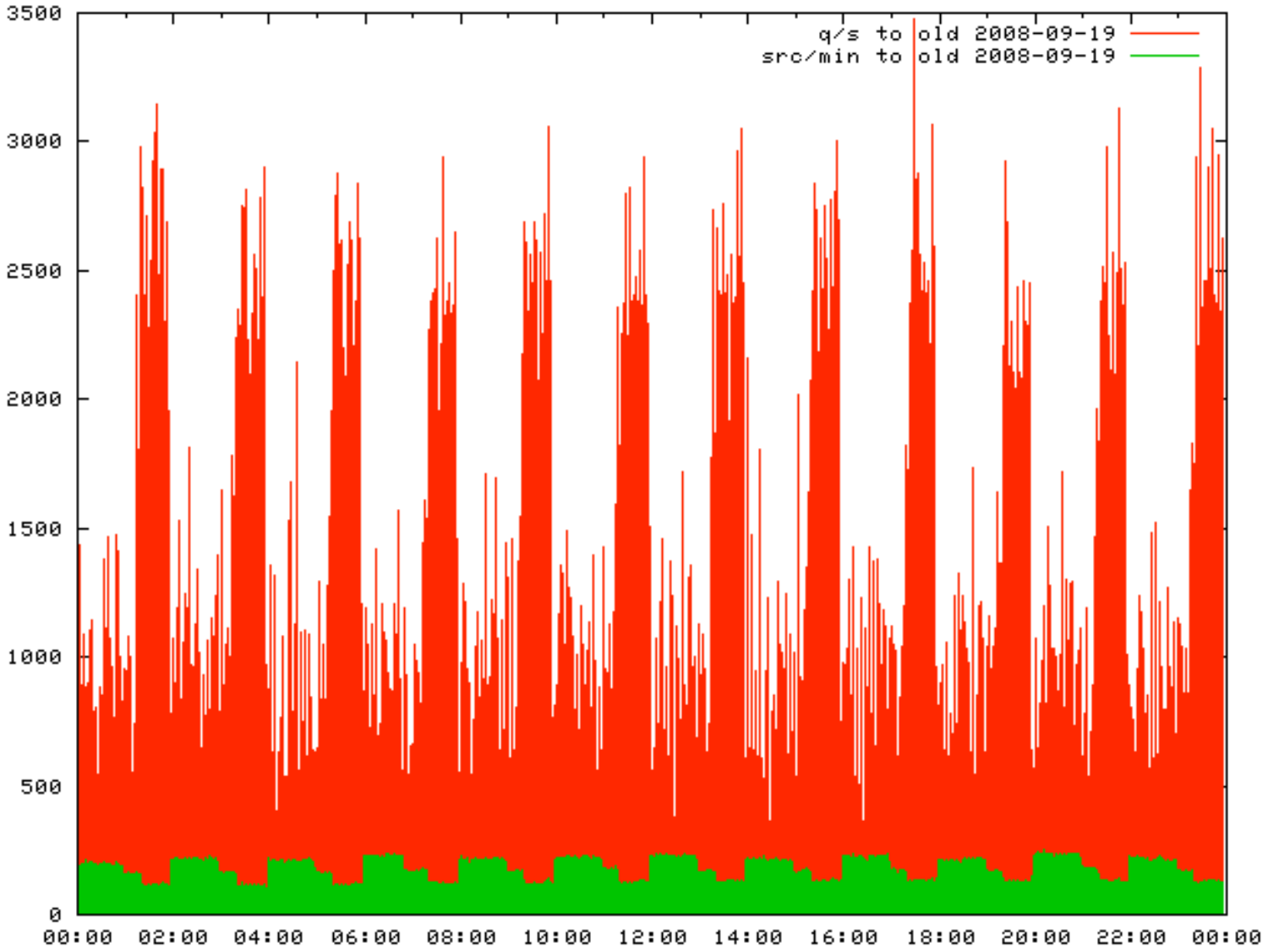
Trivia

- After seven 7 months, query rate is still high
  - Die-hard *dropcatchers*
  - Resolvers with (outdated) copies of the root zone!
    - `2006082700`
    - … or abandoned alternate root system
  - Open Recursive Name Servers
  - Weird high TTLs on TLD NS RRSet and A RRSets
    - `s.de.net.  2132443279 IN A  193.159.170.149`
  - `fpdns` identifies „non-standard“ software

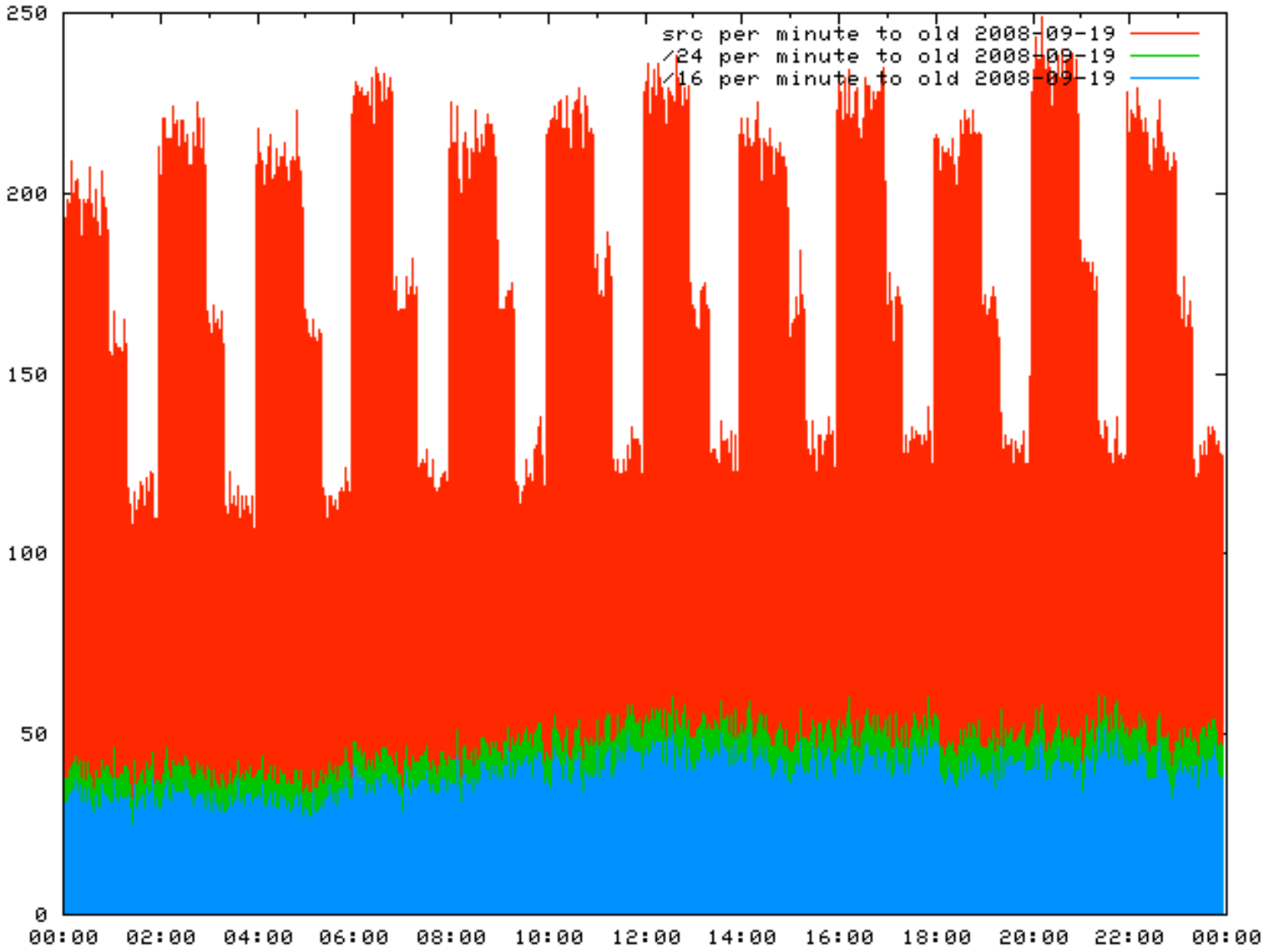
DSC 2008-04-10 -> 2008-04-12



2008-09-19 Traffic to old address



2008-09-19 Stalker distribution



Future Work

- Investigate some resolvers in more detail
  - Especially the „open“ ones
- Investigate „first contacts“
  - Early cache expiry?
  - No cache at all?
- Redo experiment with different server name
  - Within `nic.de`

?/!

Peter Koch, DENIC eG

<koch@denic.de>
<http://www.denic.de>