Bond
Internet Systems

RESOLVER TRAFFIC: WHAT DOES IT LOOK LIKE?

João Damas

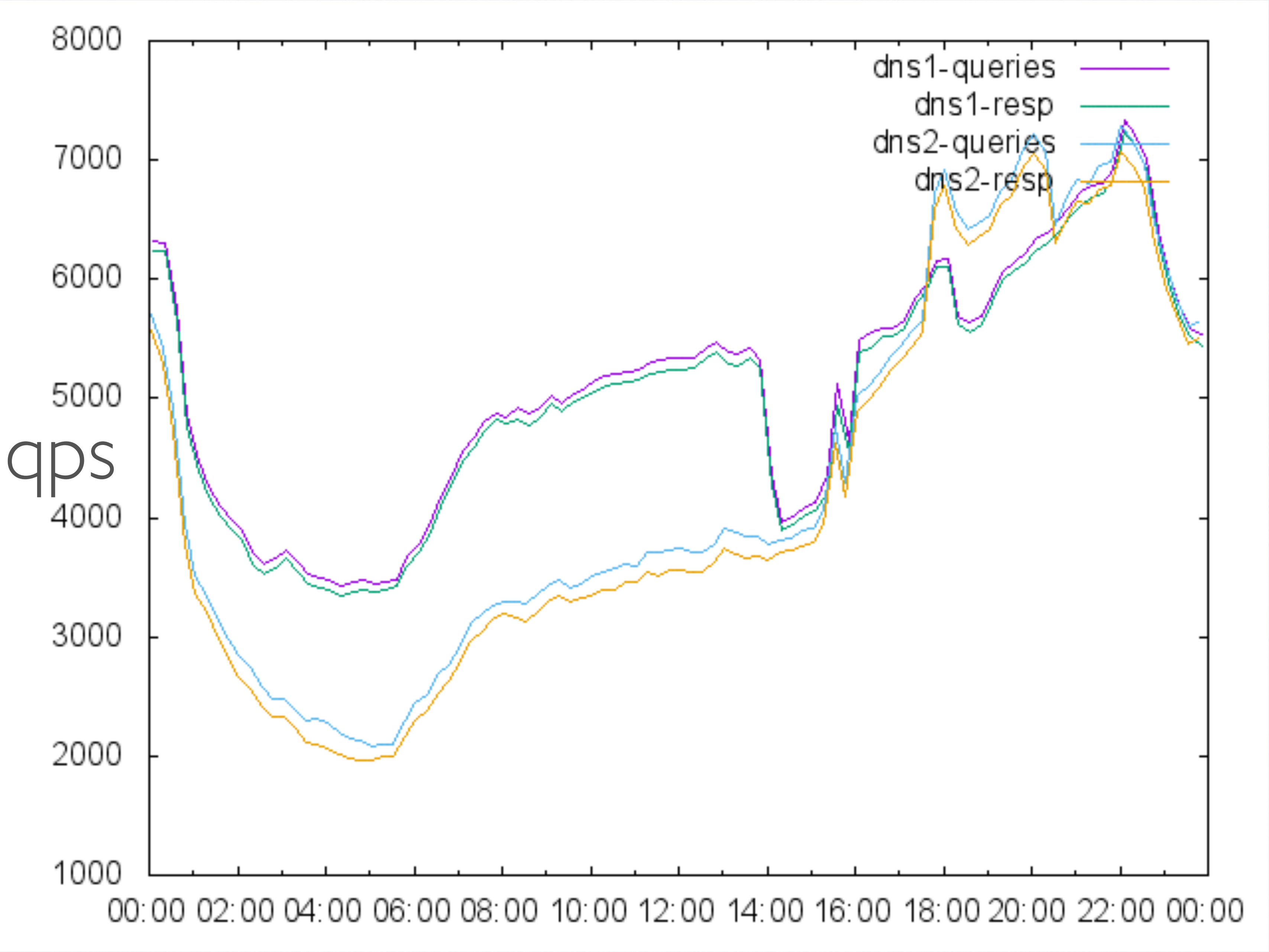
Background

- We look a lot at traffic between resolvers and authoritative servers
- and very little at traffic between recursive resolvers and they clients.
- Is it still the Internet? or maybe something similar to the Internet?

Where is the data?

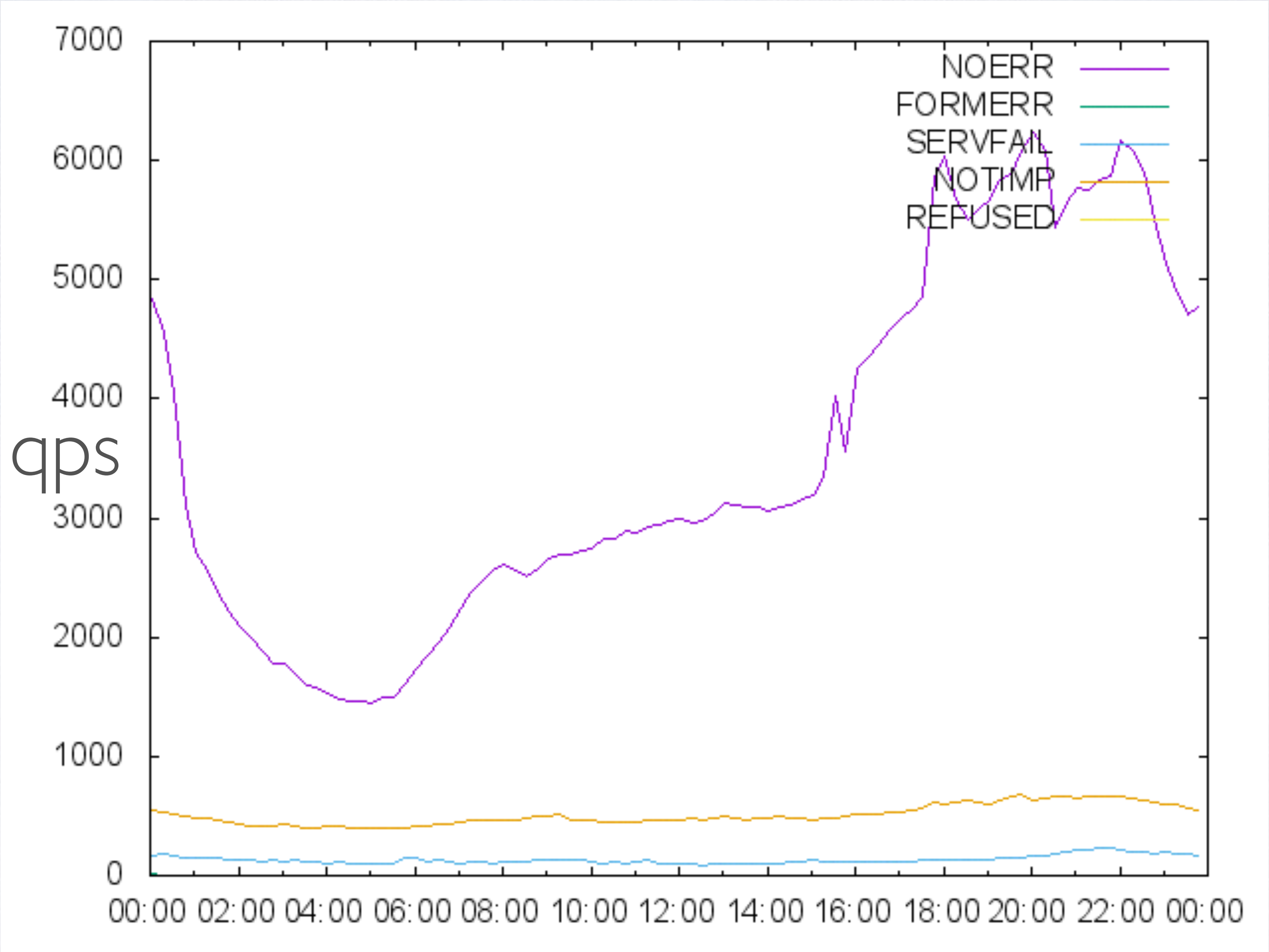
- Hard to get a hold of this sort of traffic
- Concerns about PII, exposing customer issues, etc

The sample

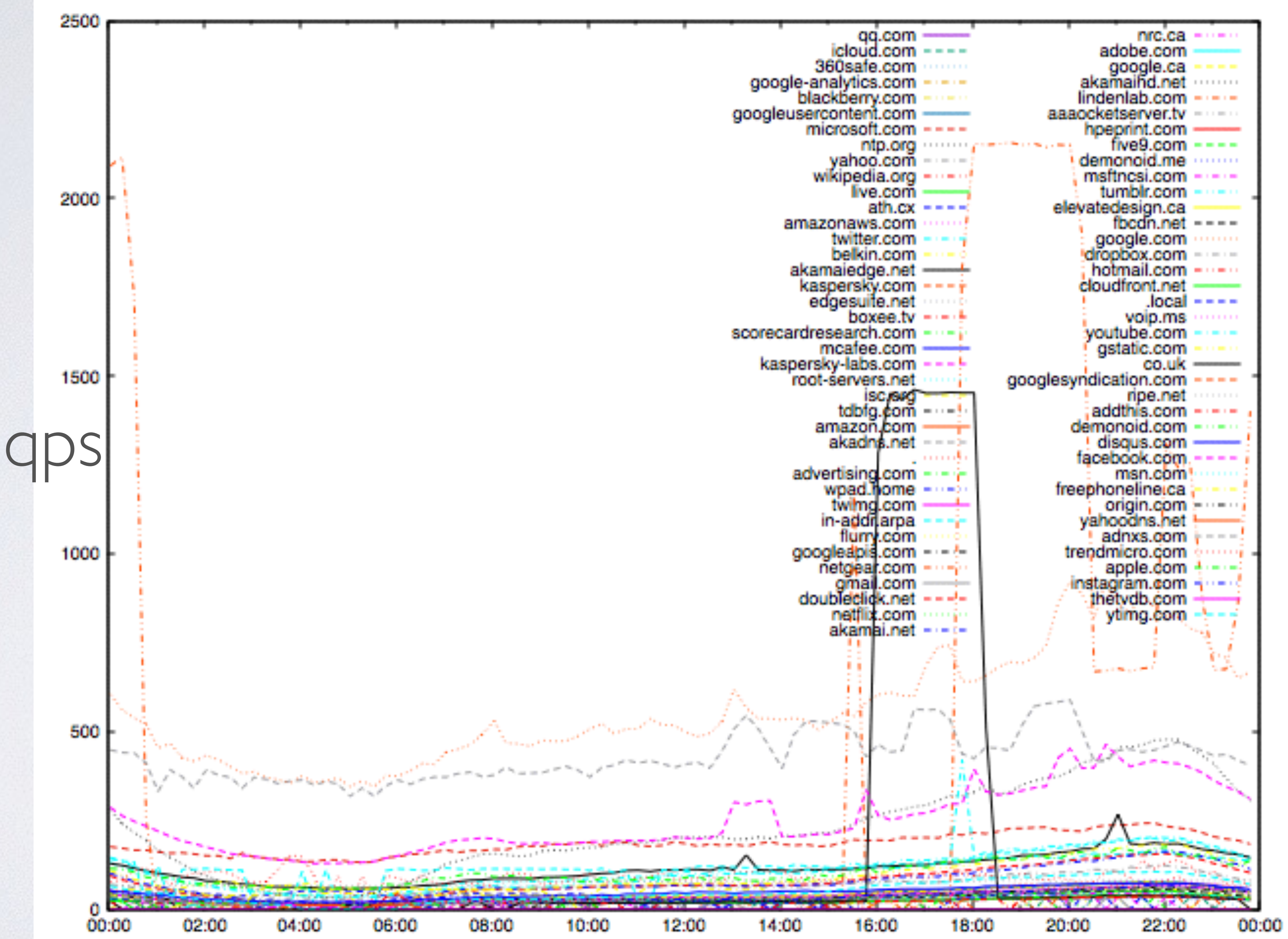

qps
8000
7000
6000
5000
4000
3000
2000
1000
00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 00:00
dns1-queries
dns1-resp
dns2-queries
dns2-resp

Bond Internet Systems

RCODE distribution

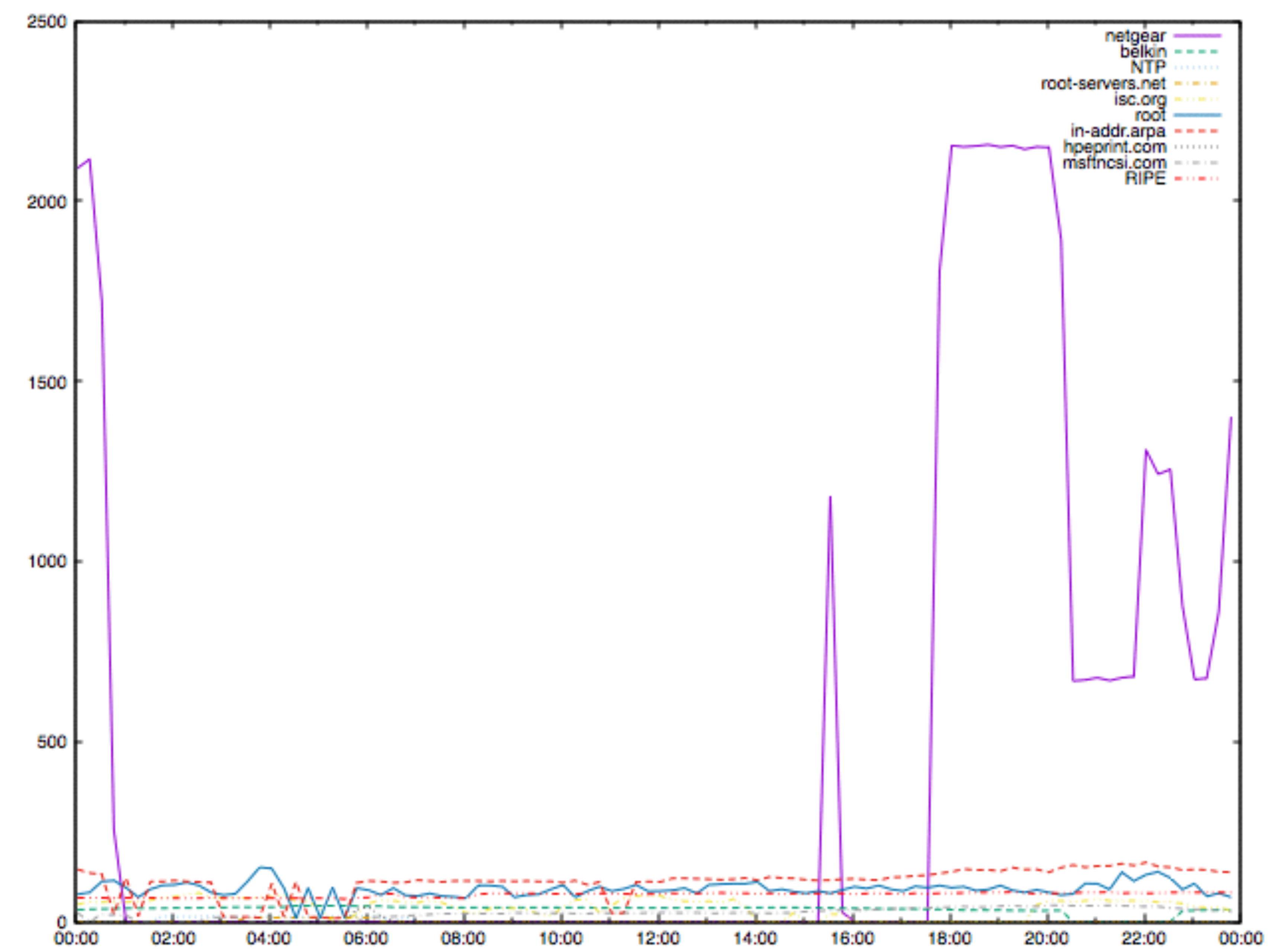


Domains

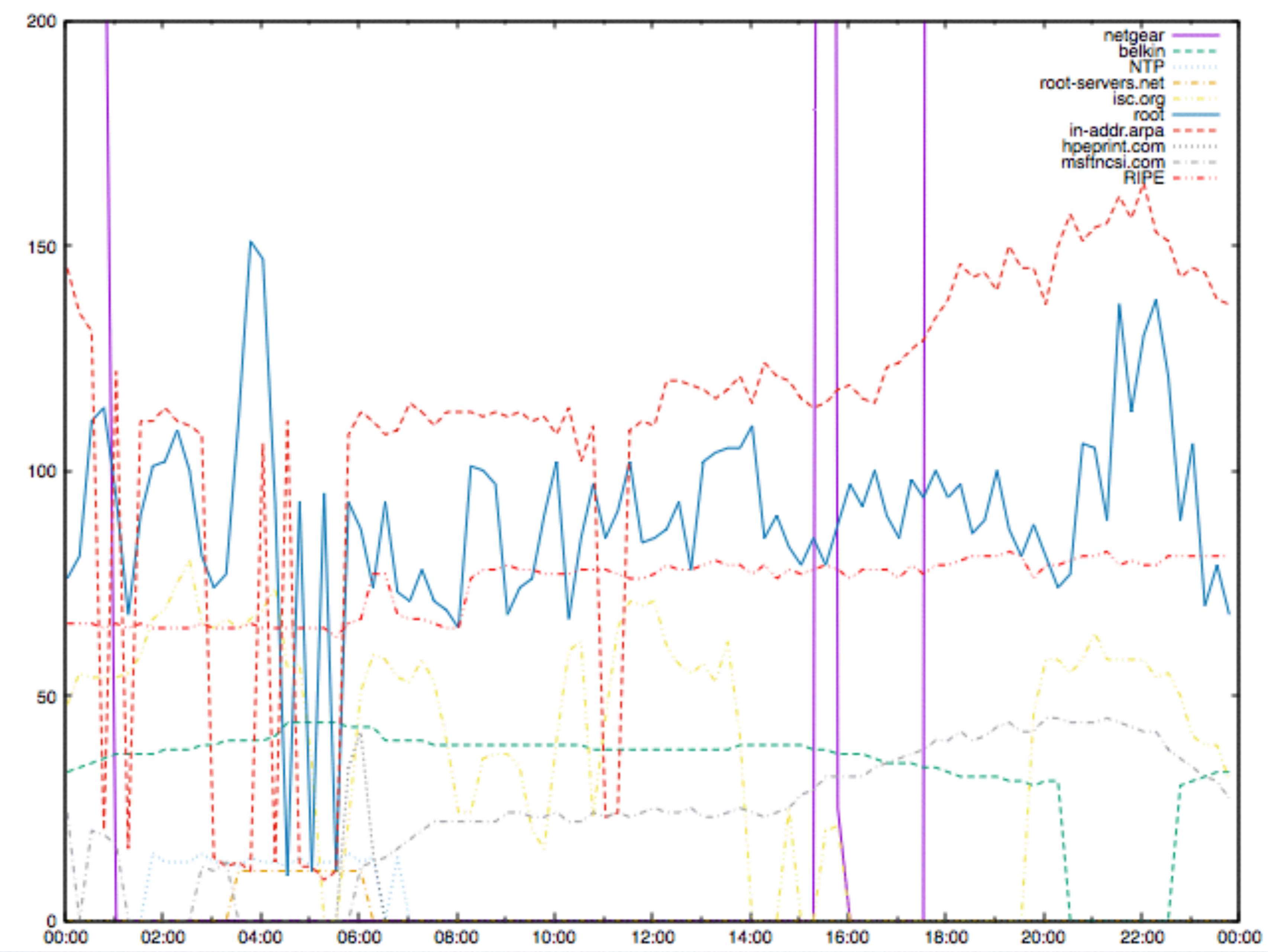

qps
2500
2000
1500
1000
500
0
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
qq.com
icloud.com
360safe.com
google-analytics.com
blackberry.com
googleusercontent.com
microsoft.com
ntp.org
yahoo.com
wikipedia.org
live.com
ath.cx
amazonaws.com
twitter.com
belkin.com
akamaiedge.net
kaspersky.com
edgesuite.net
boxee.tv
scorecardresearch.com
mcafee.com
kaspersky-labs.com
root-servers.net
isc.org
tdbfg.com
amazon.com
akadns.net
advertising.com
wpad.home
twimg.com
in-addr.arpa
flurry.com
googleapis.com
netgear.com
gmail.com
doubleclick.net
netflix.com
akamai.net
nrc.ca
adobe.com
google.ca
akamaihd.net
lindenlab.com
aaaocketserver.tv
hpeprint.com
five9.com
demonoid.me
msftncsi.com
tumblr.com
elevatedesign.ca
fbcdn.net
google.com
dropbox.com
hotmail.com
cloudfront.net
.local
voip.ms
youtube.com
gstatic.com
co.uk
googlesyndication.com
ripe.net
addthis.com
demonoid.com
disqus.com
facebook.com
msn.com
freephoneline.ca
origin.com
yahoodns.net
adnxs.com
trendmicro.com
apple.com
instagram.com
thetvdb.com
ytimg.com

Bond
Internet Systems

Infrastructure domains



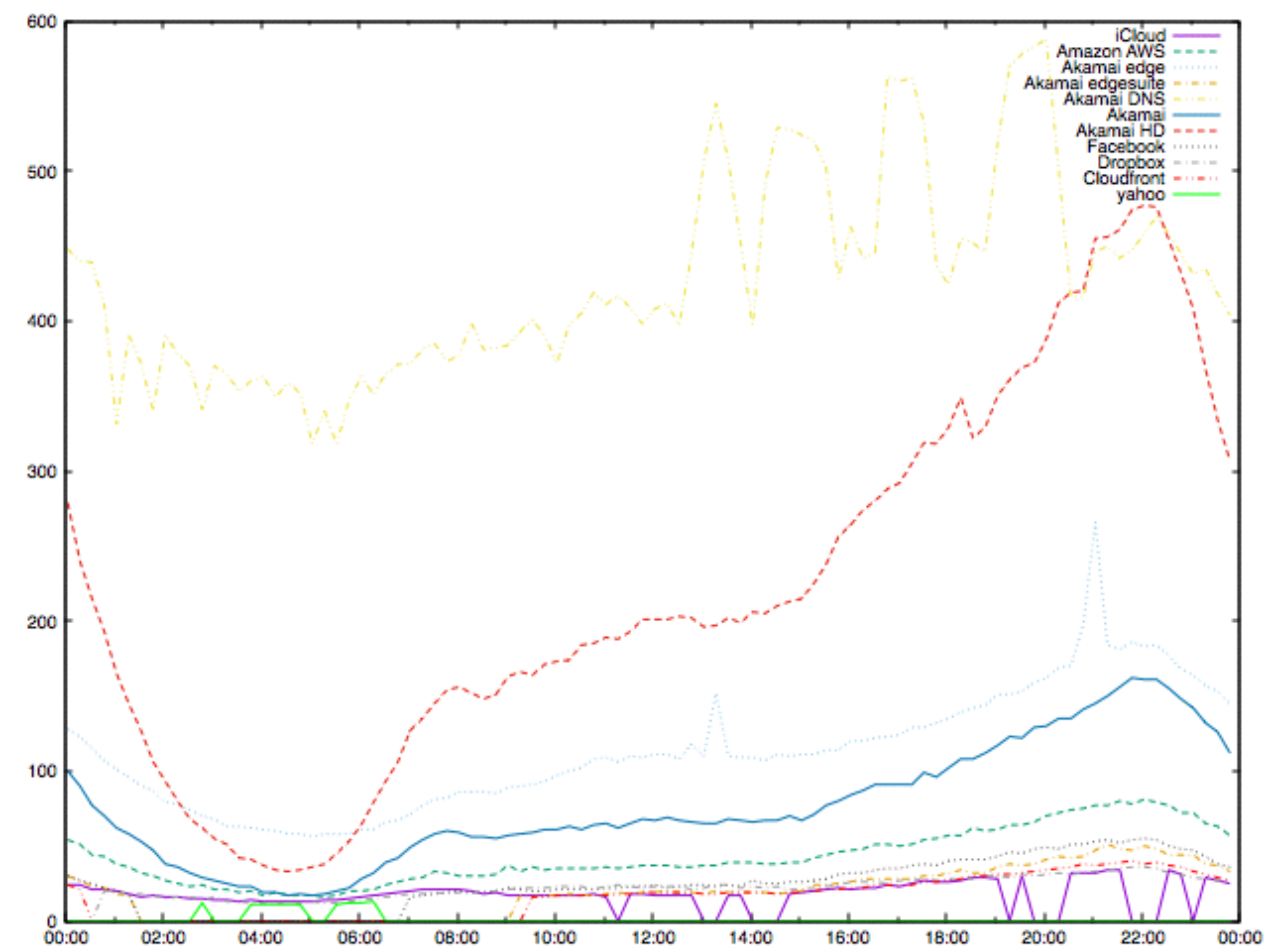
Infrastructure domains zoom



Bond

Internet Systems

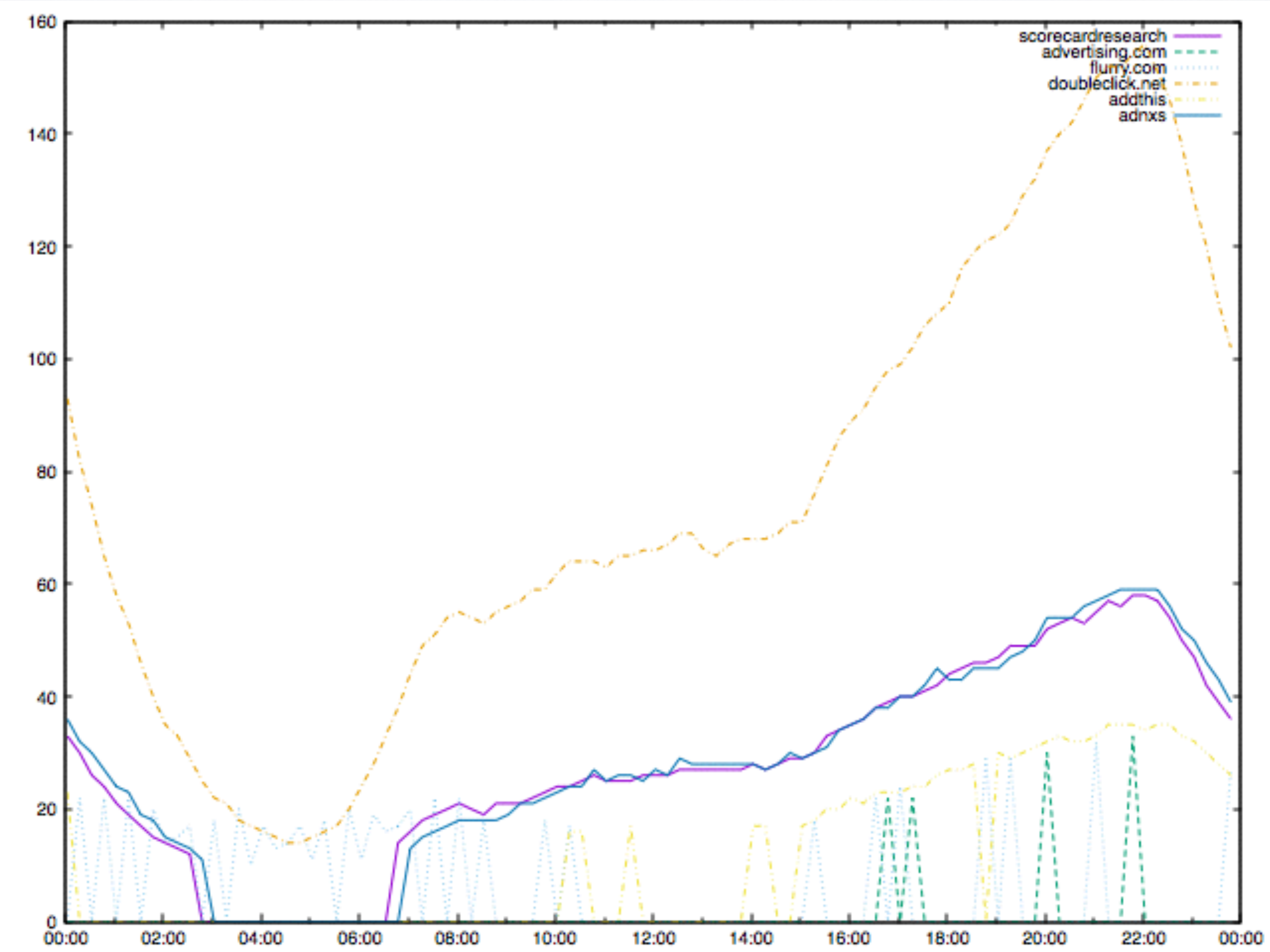
CDNs



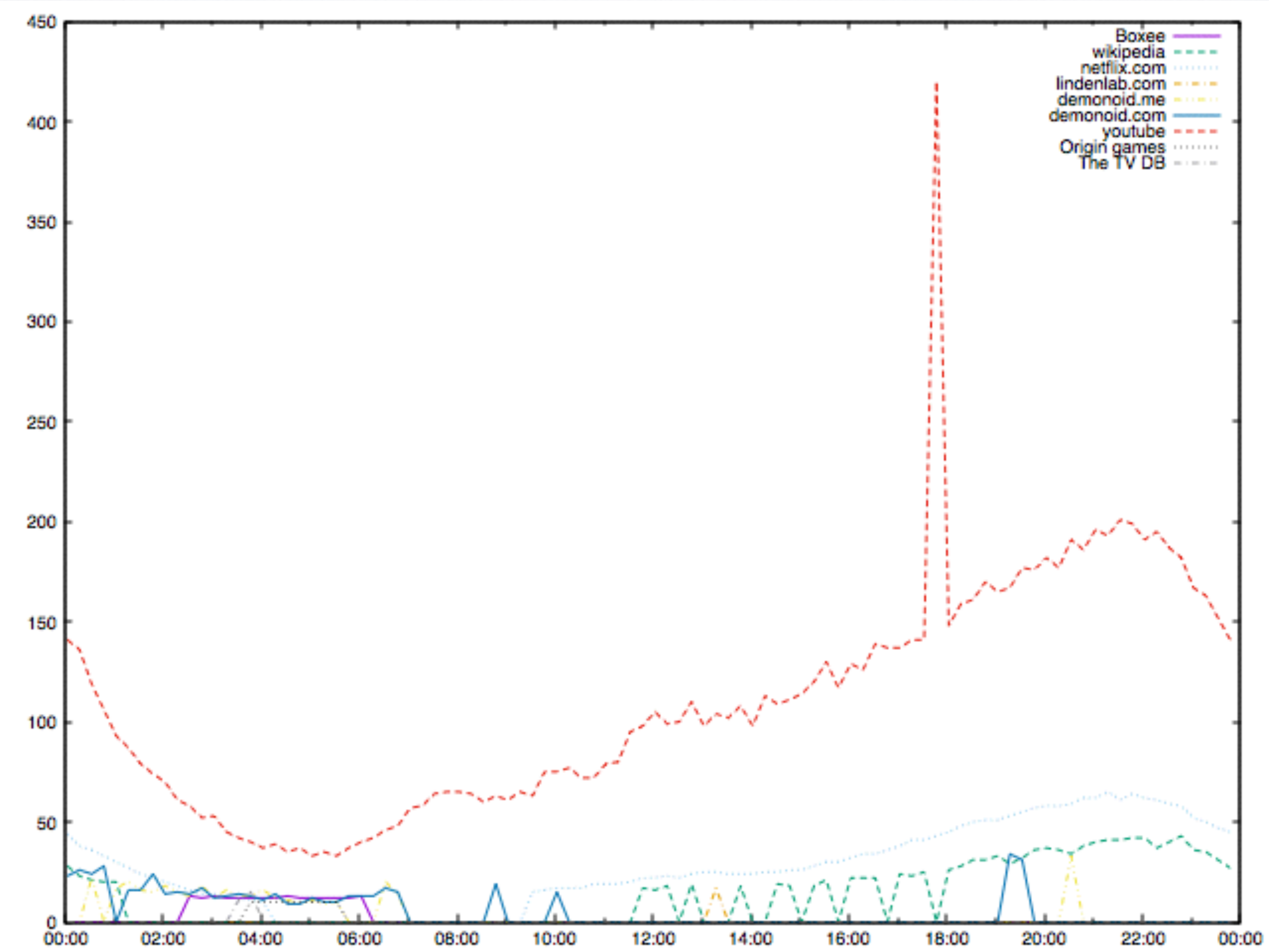
Bond

Internet Systems

ADs

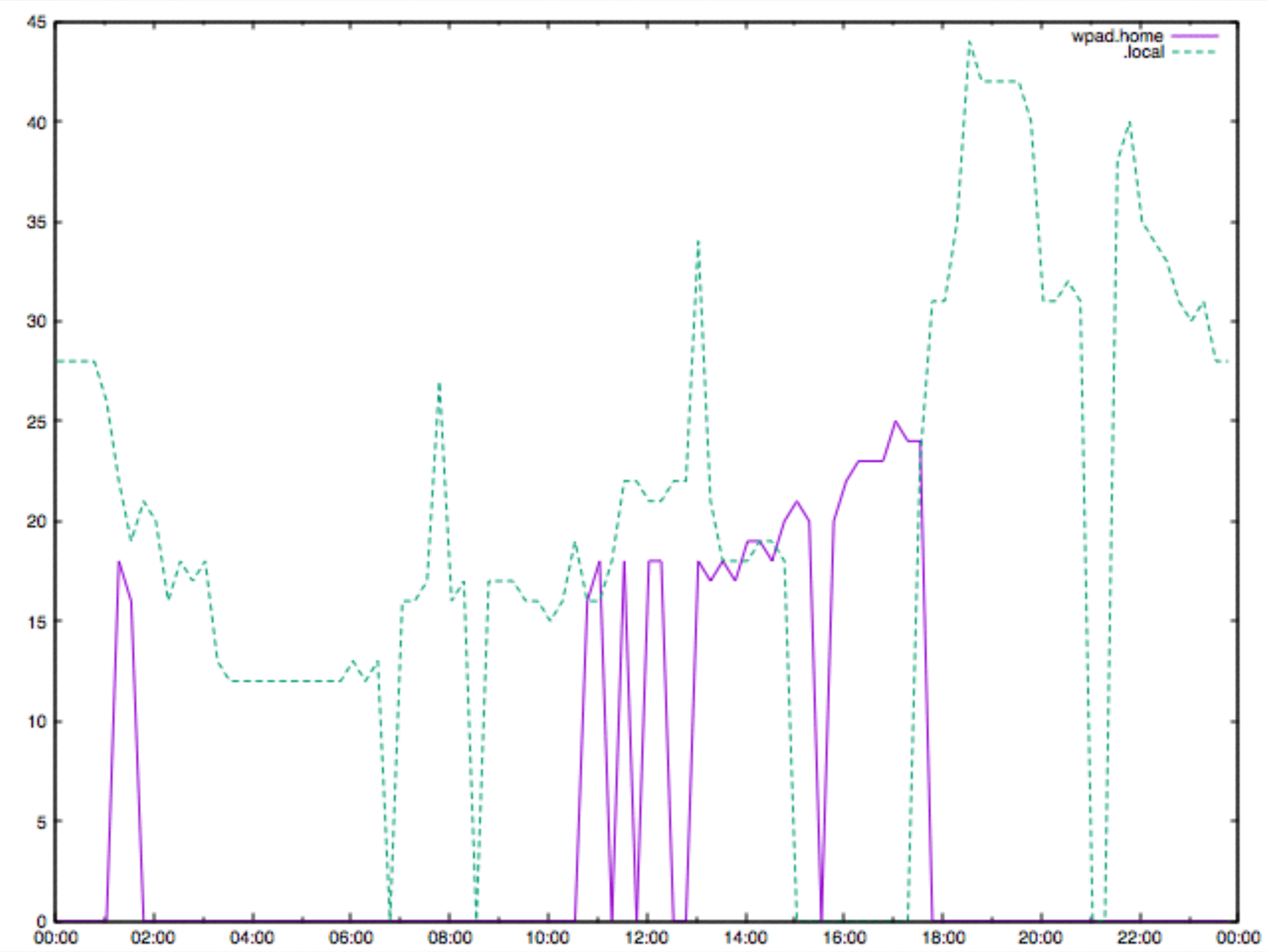


Entertainment sites



Bond
Internet Systems

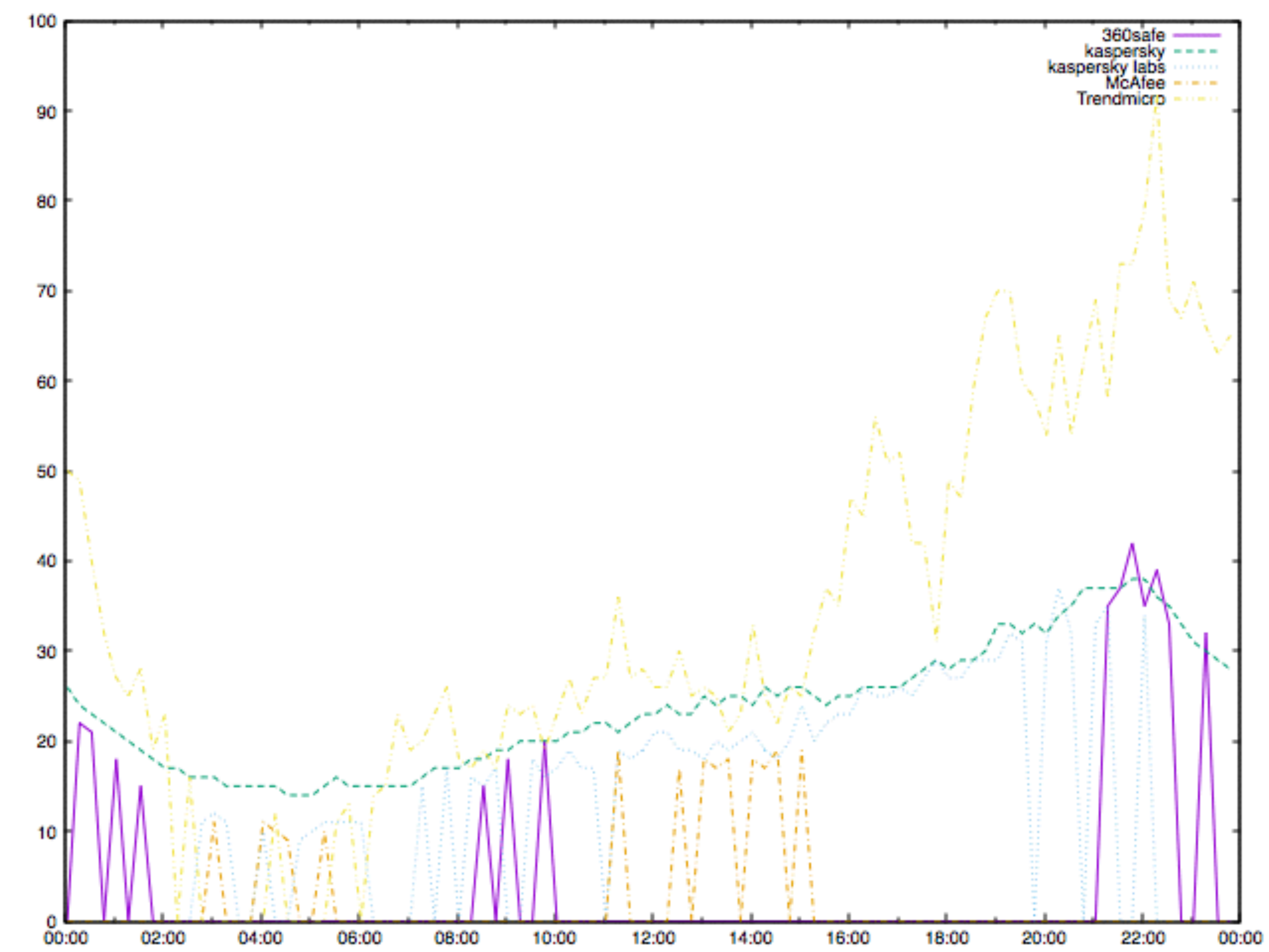
wtf sites



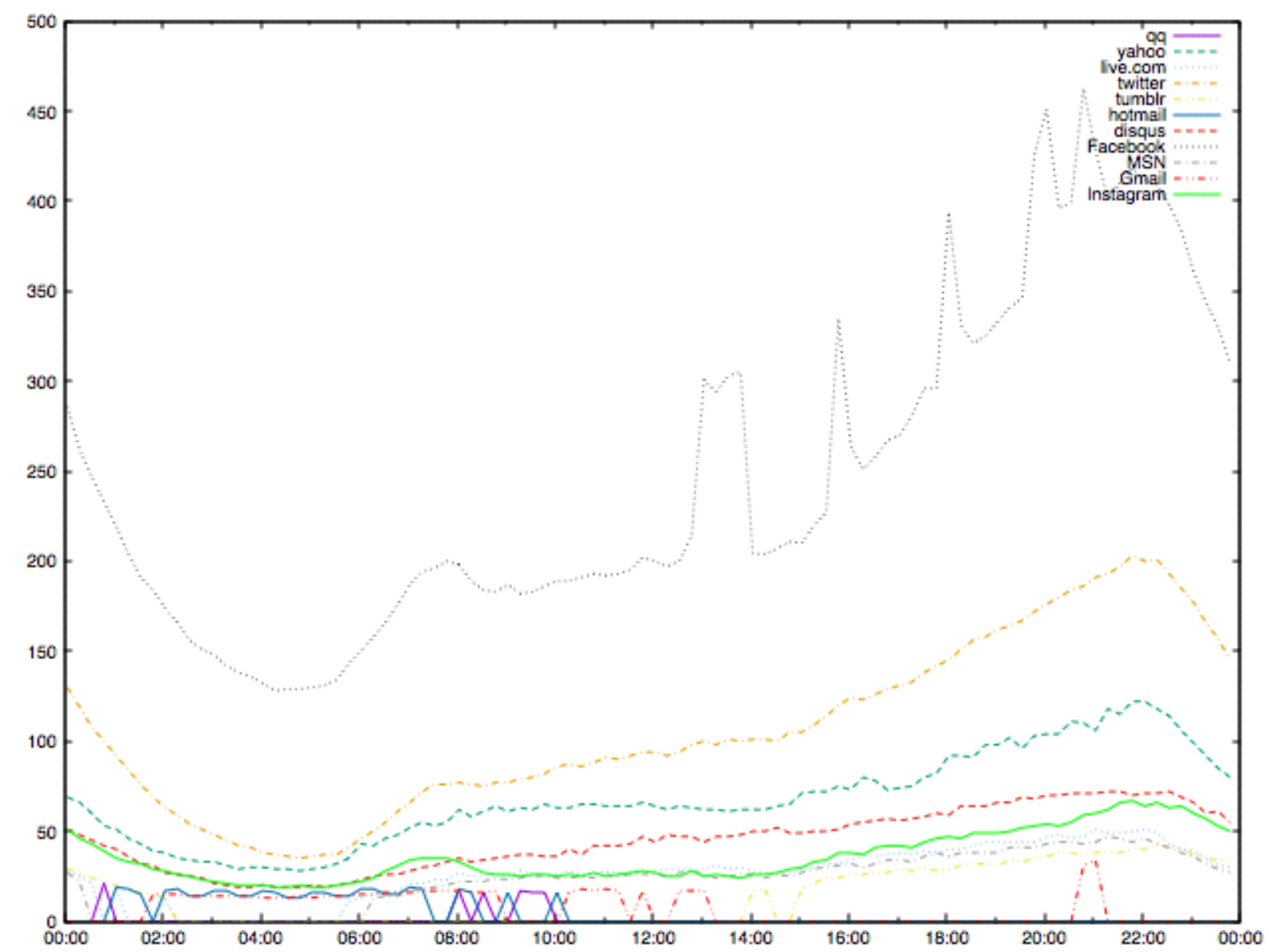
Bond

Internet Systems

Security services



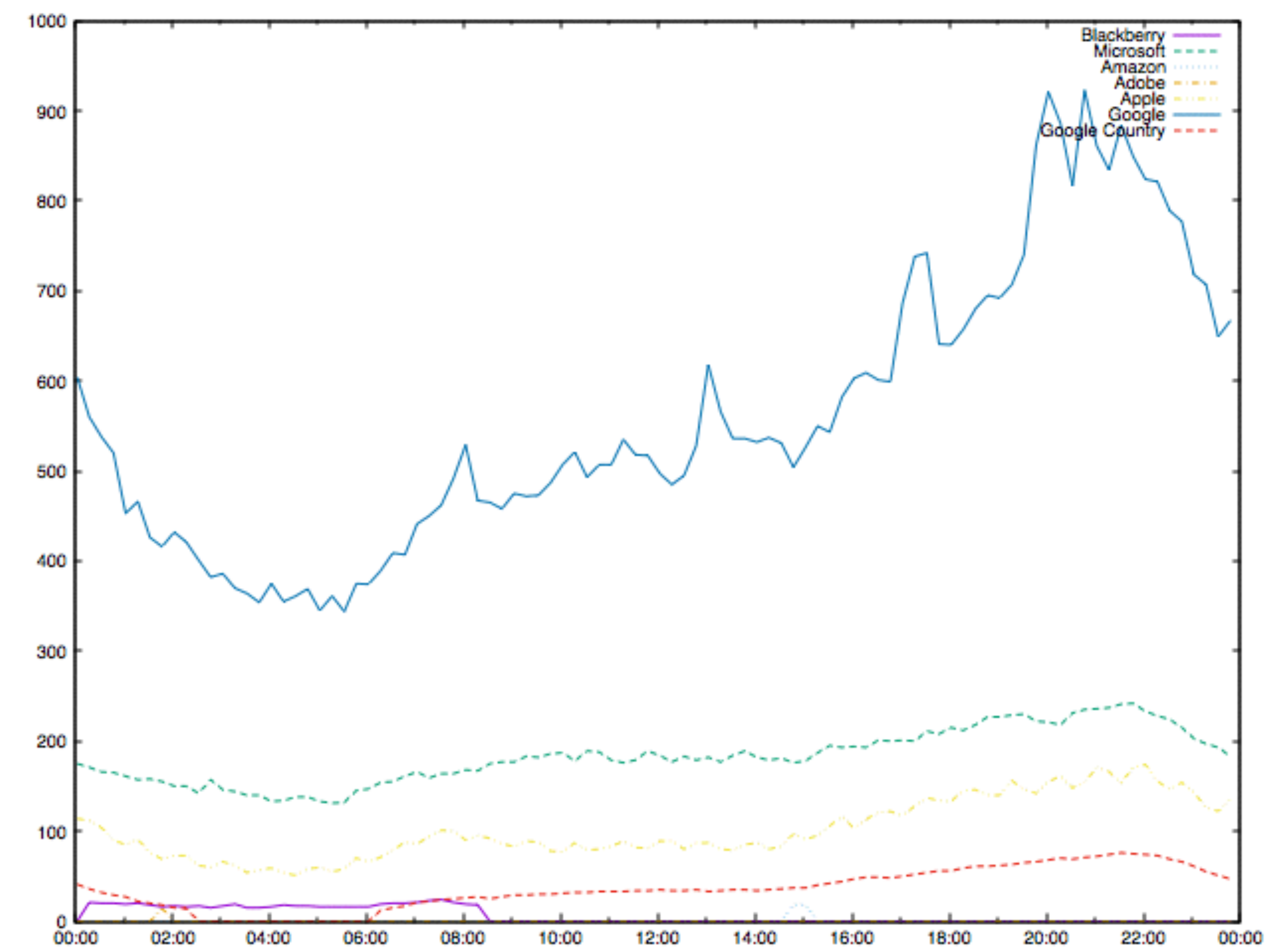
Social



500
450
400
350
300
250
200
150
100
50
0
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
qq
yahoo
live.com
twitter
tumblr
hotmail
disqus
Facebook
MSN
Gmail
Instagram

Bond
Internet Systems

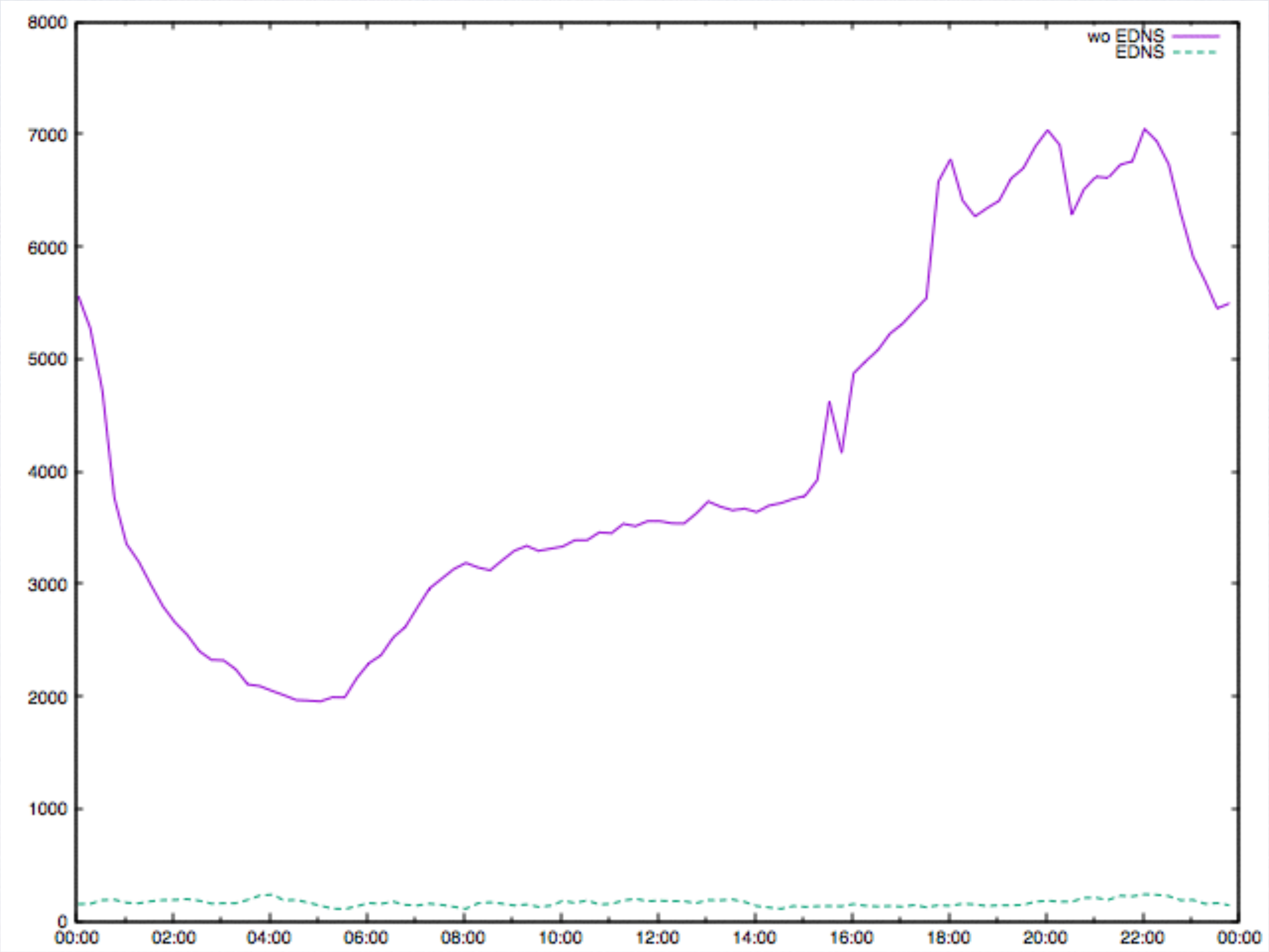
Main domains



Bond

Internet Systems

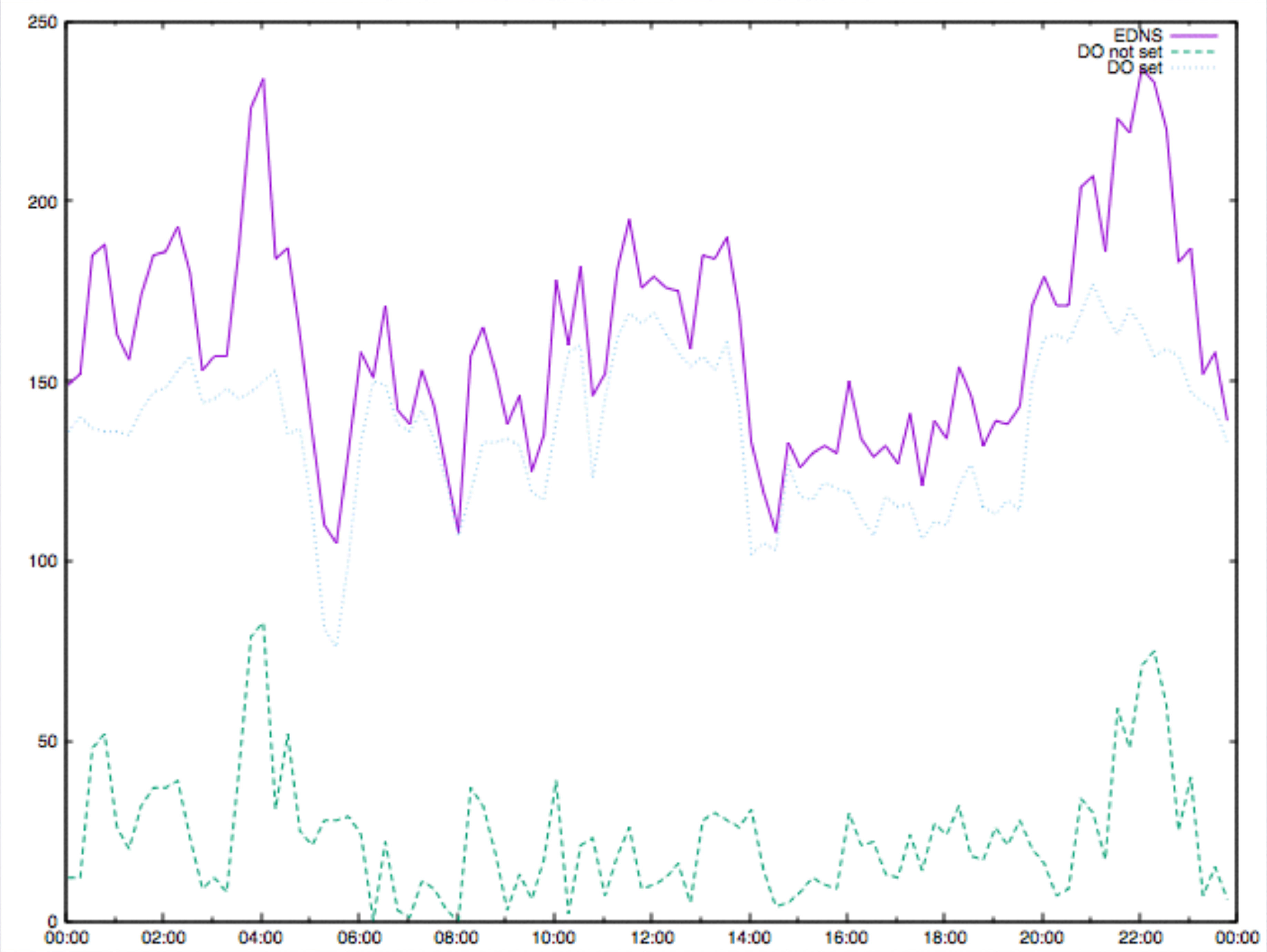
EDNS usage



Bond

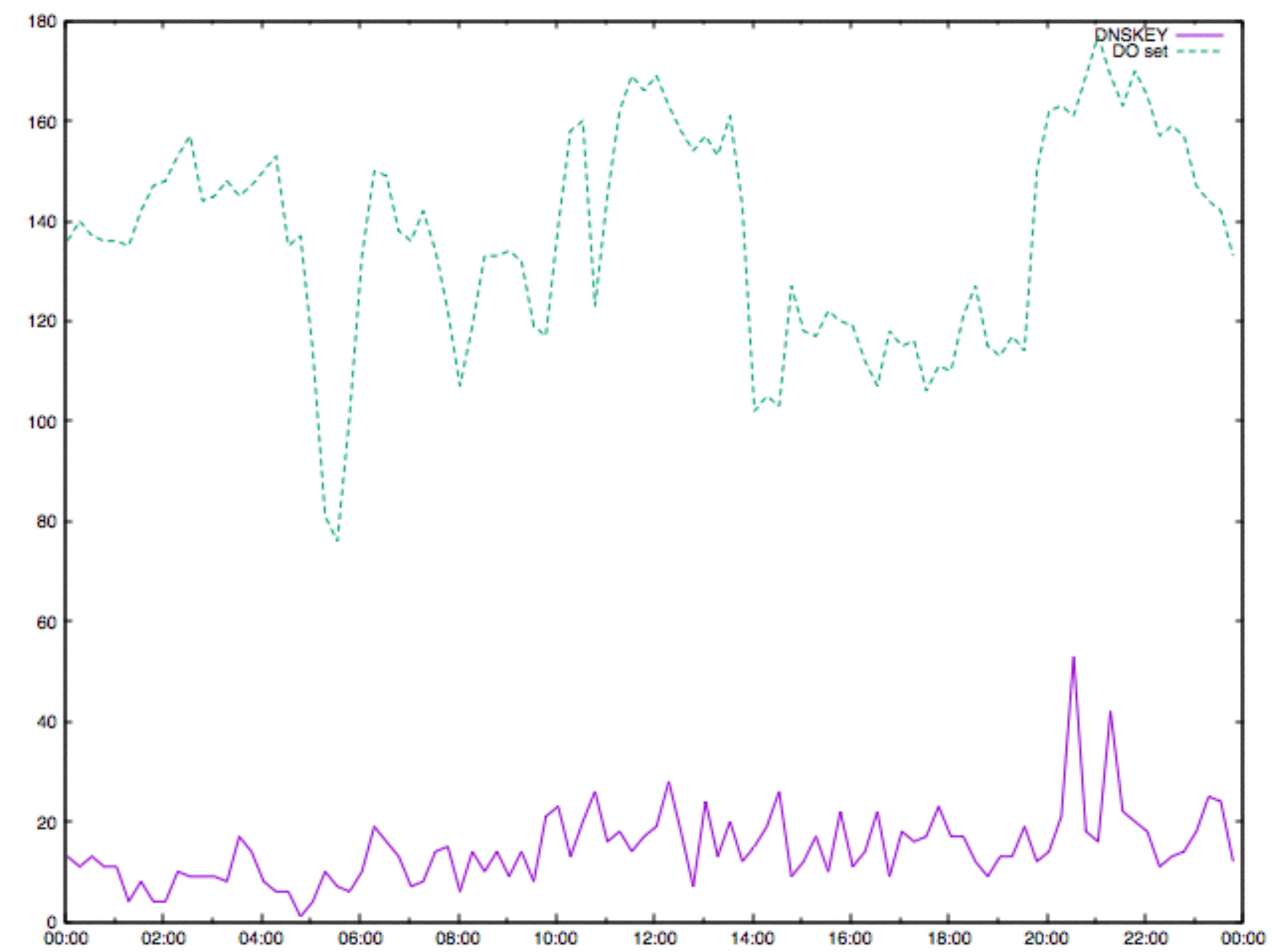
Internet Systems

DNSSEC - do



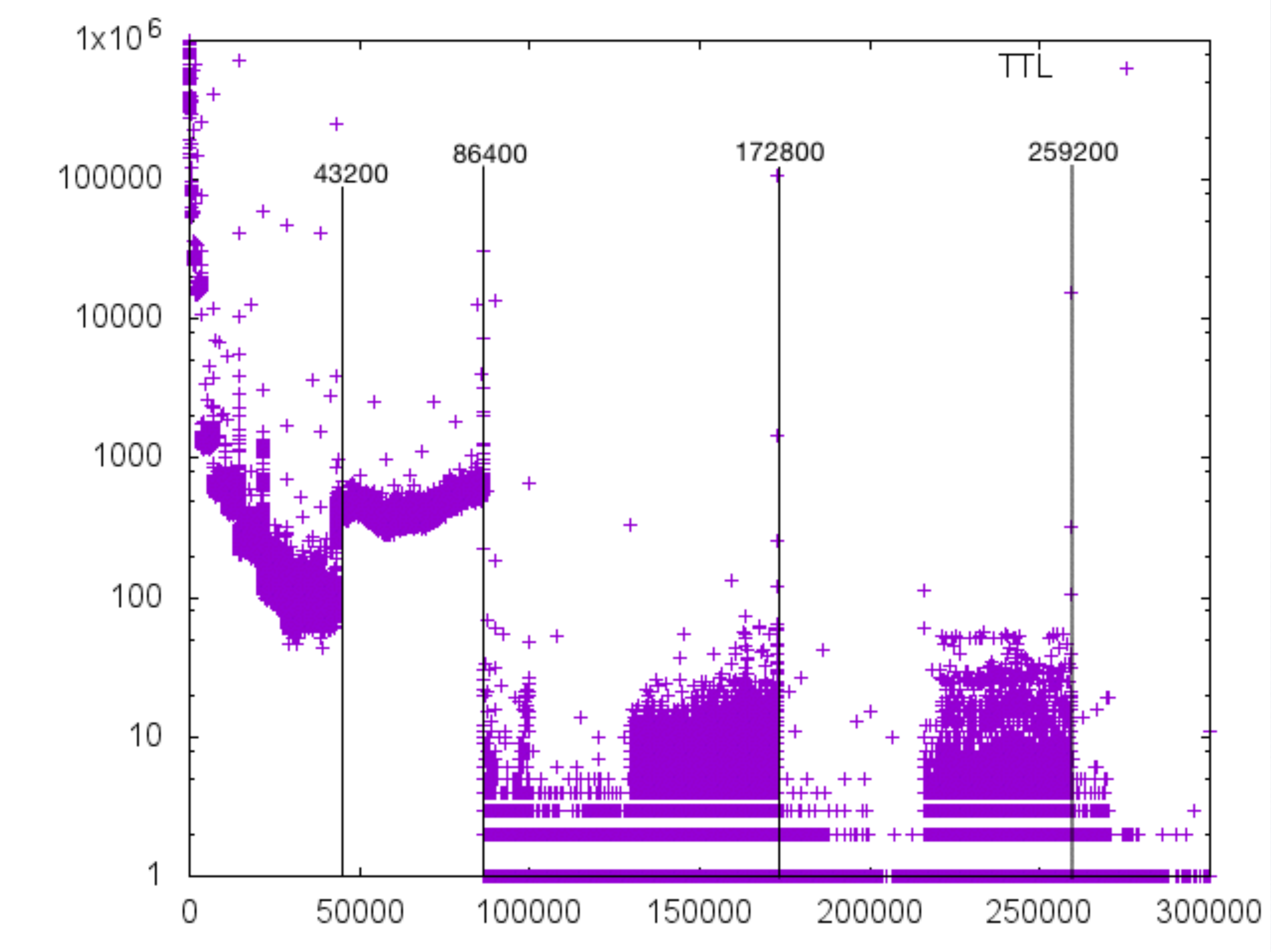
Bond
Internet Systems

DNSSEC - dnskey



Bond
Internet Systems

TTL



What now?

- Study how parameter changes at resolves affect their behaviour towards clients
- Followup work: study impact of changes in server configuration and actions on load handling
  - how does min_ttl help/harm
  - can prefetch help? When and how?

Acknowledgements

This study was sponsored by a Comcast research grant

Questions?