Bond
Internet Systems

RESOLVER TRAFFIC: WHAT DOES IT LOOK LIKE?

João Damas
Mónica Cortés Sack

Bond

Internet Systems

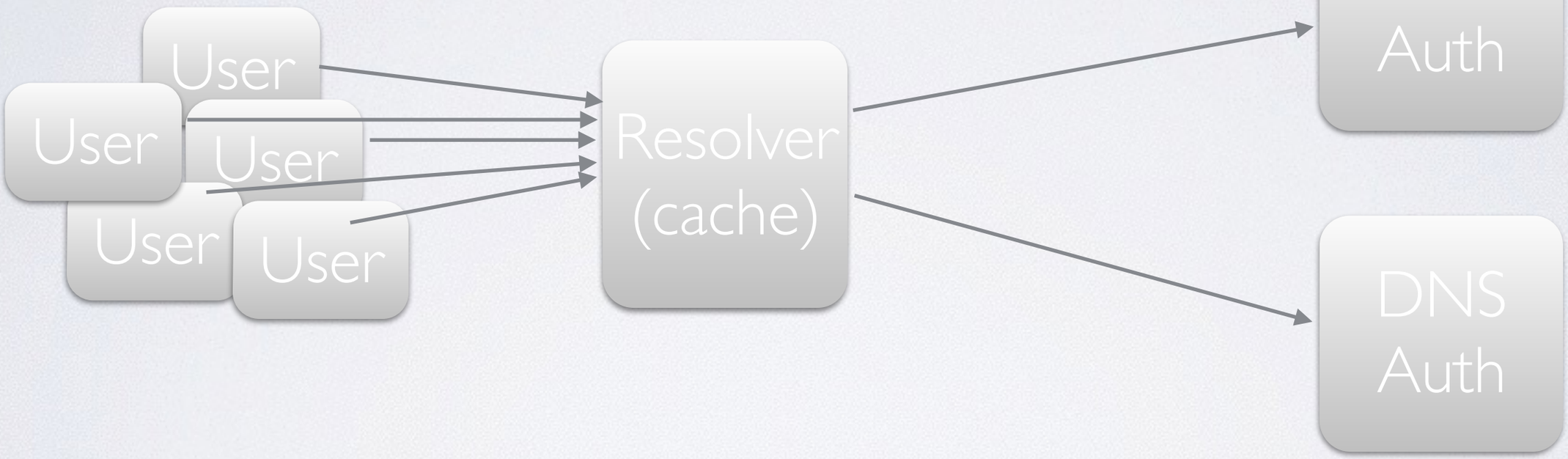
Background

- 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?

Bond

Internet Systems

What traffic we are looking at



Bond

Internet Systems

Where is the data?

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

Bond
Internet Systems

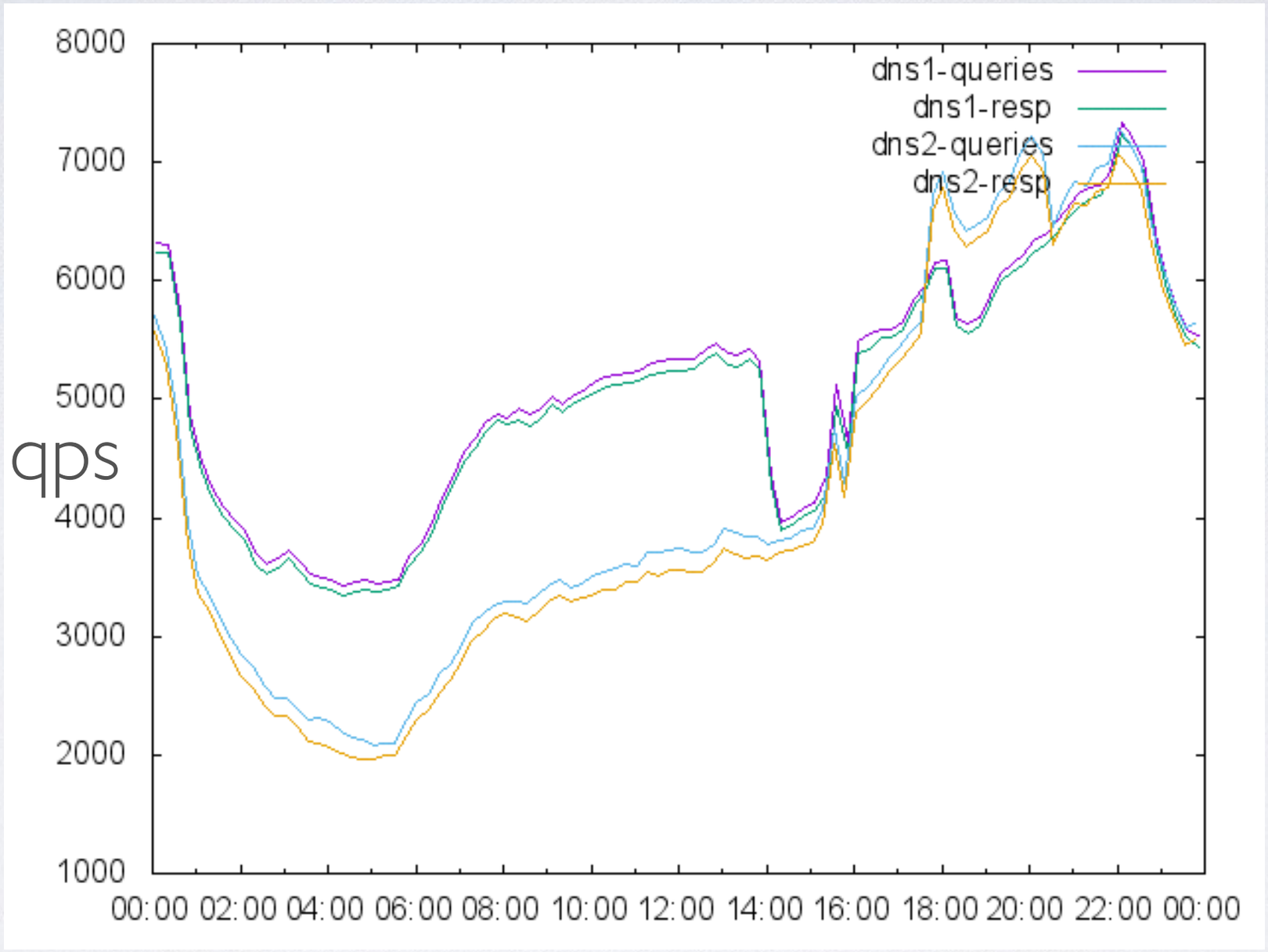
How to look at the data

- PacketQ is an excellent tool
  - no longer maintained as open source but works for 90% of your needs
- Additional home-grown software to do the remaining analysis

Bond

Internet Systems

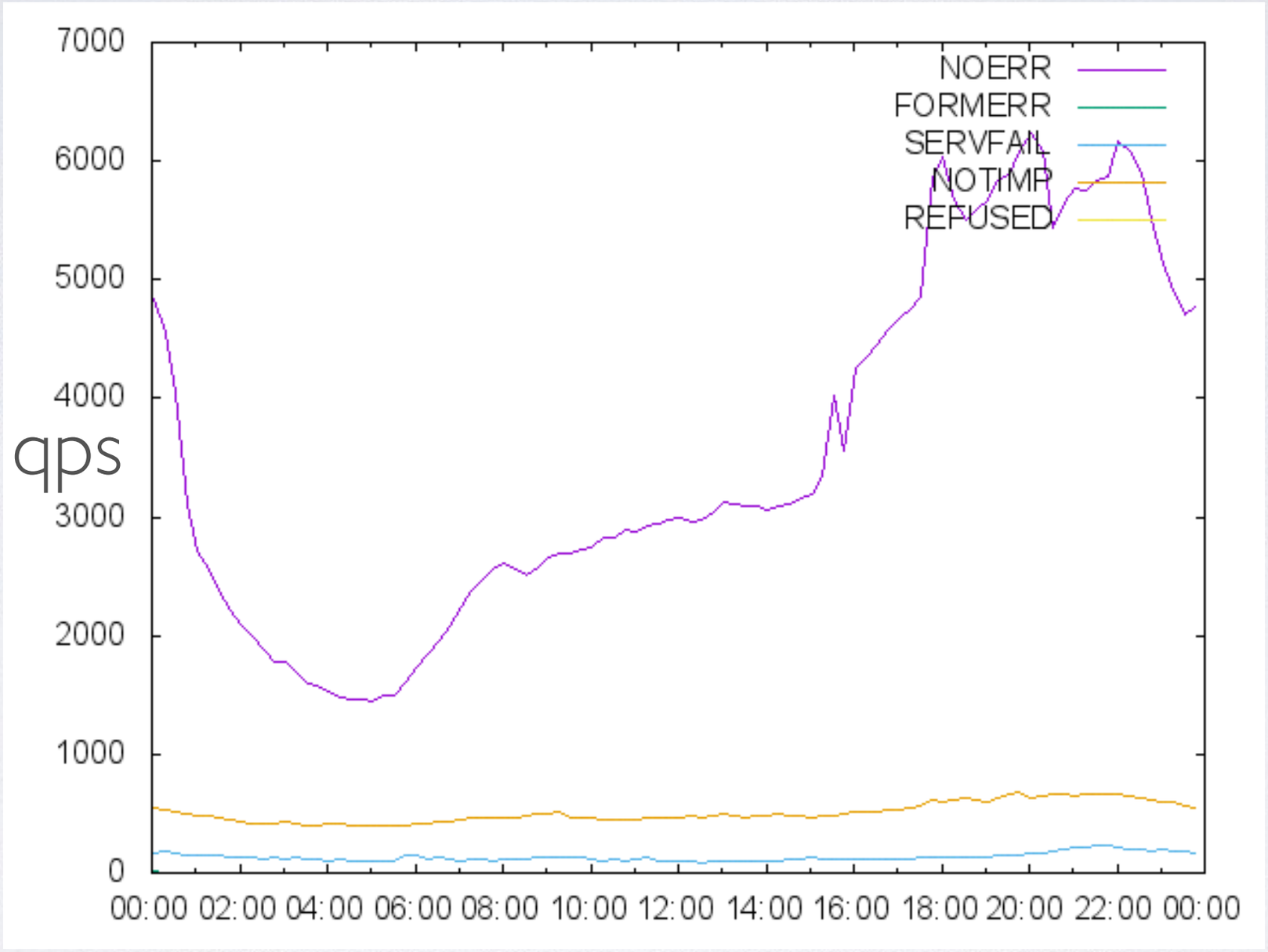
The sample



Bond

Internet Systems

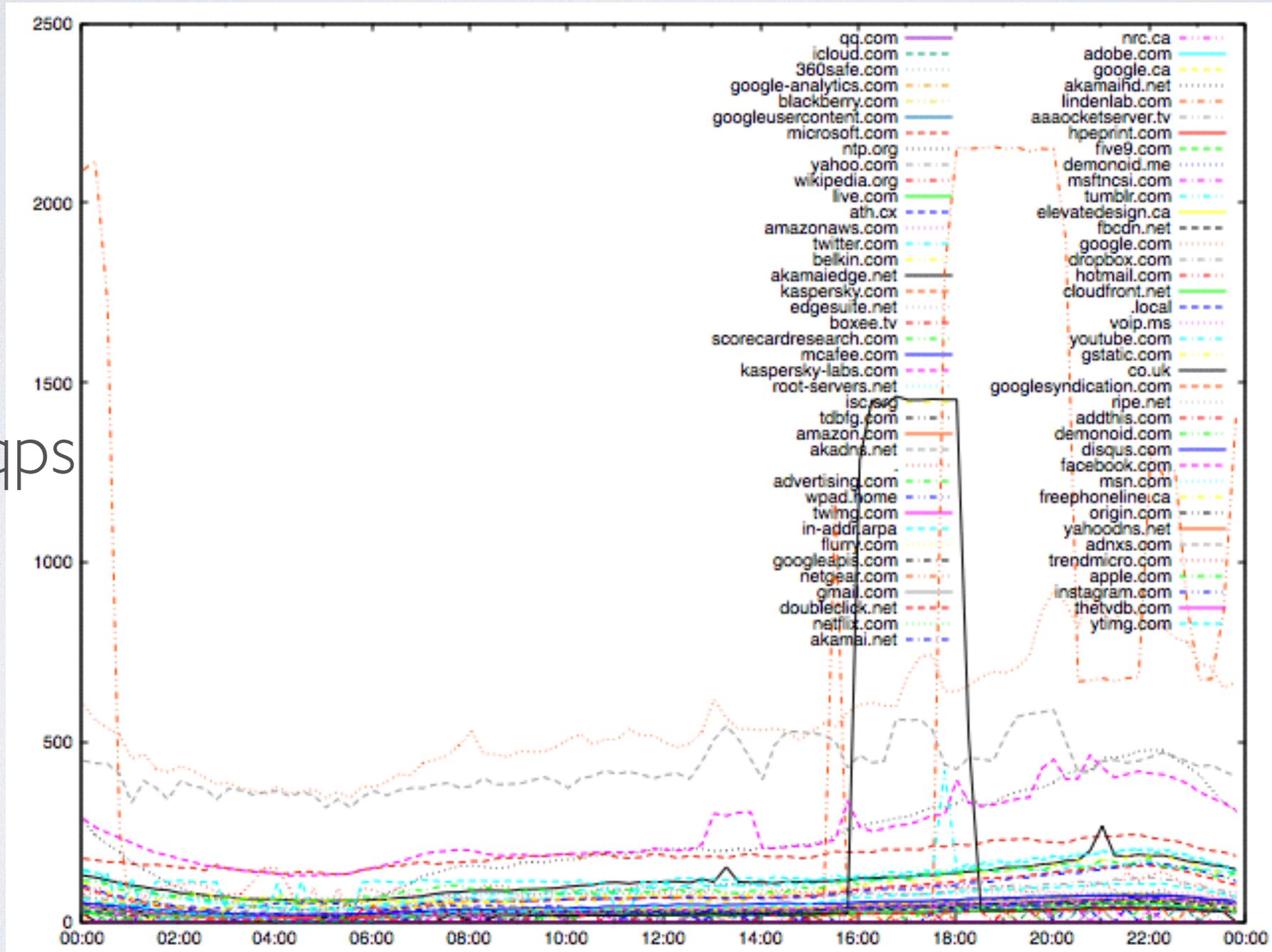
RCODE distribution



Bond

Internet Systems

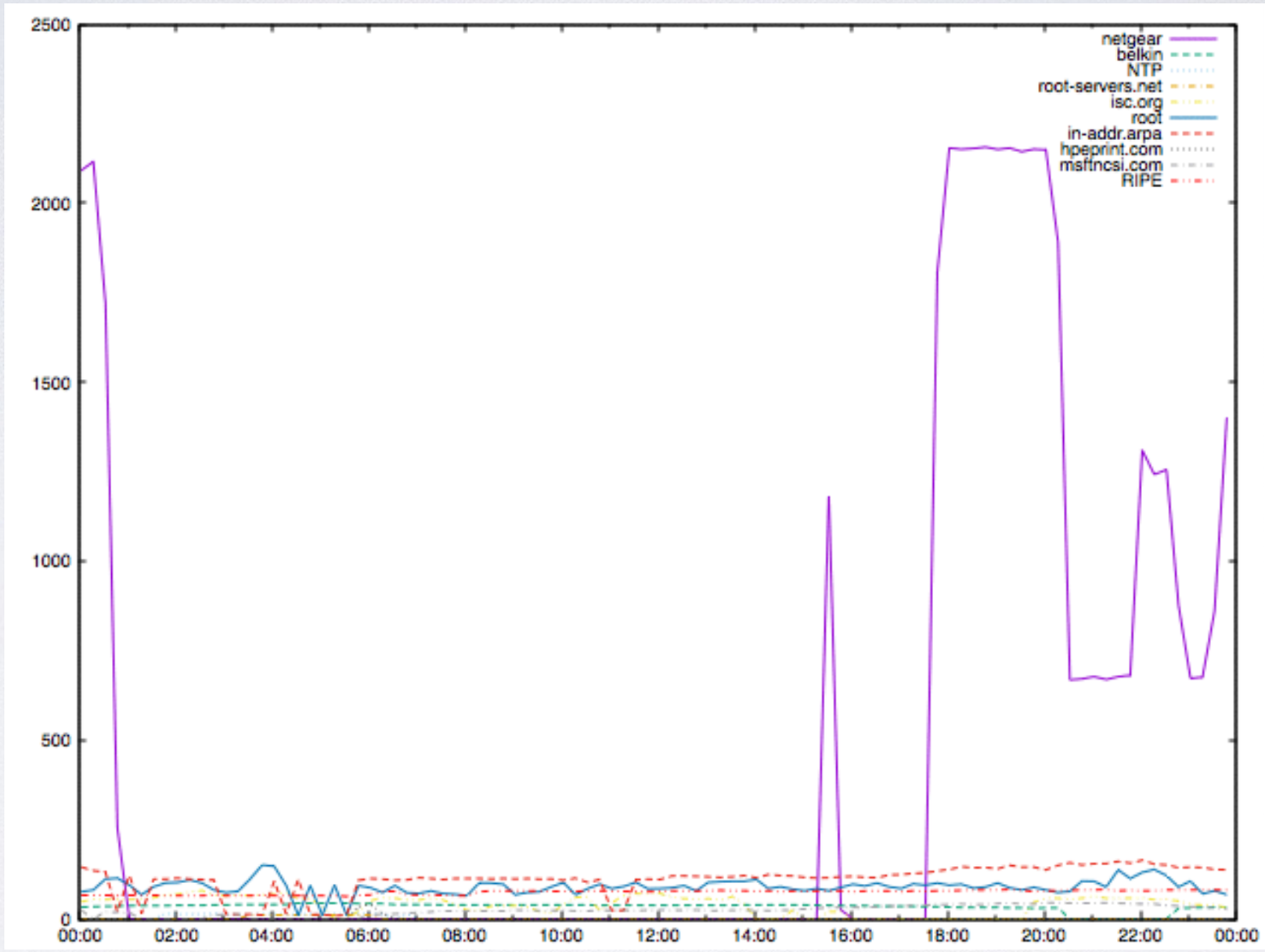
Domains



Bond

Internet Systems

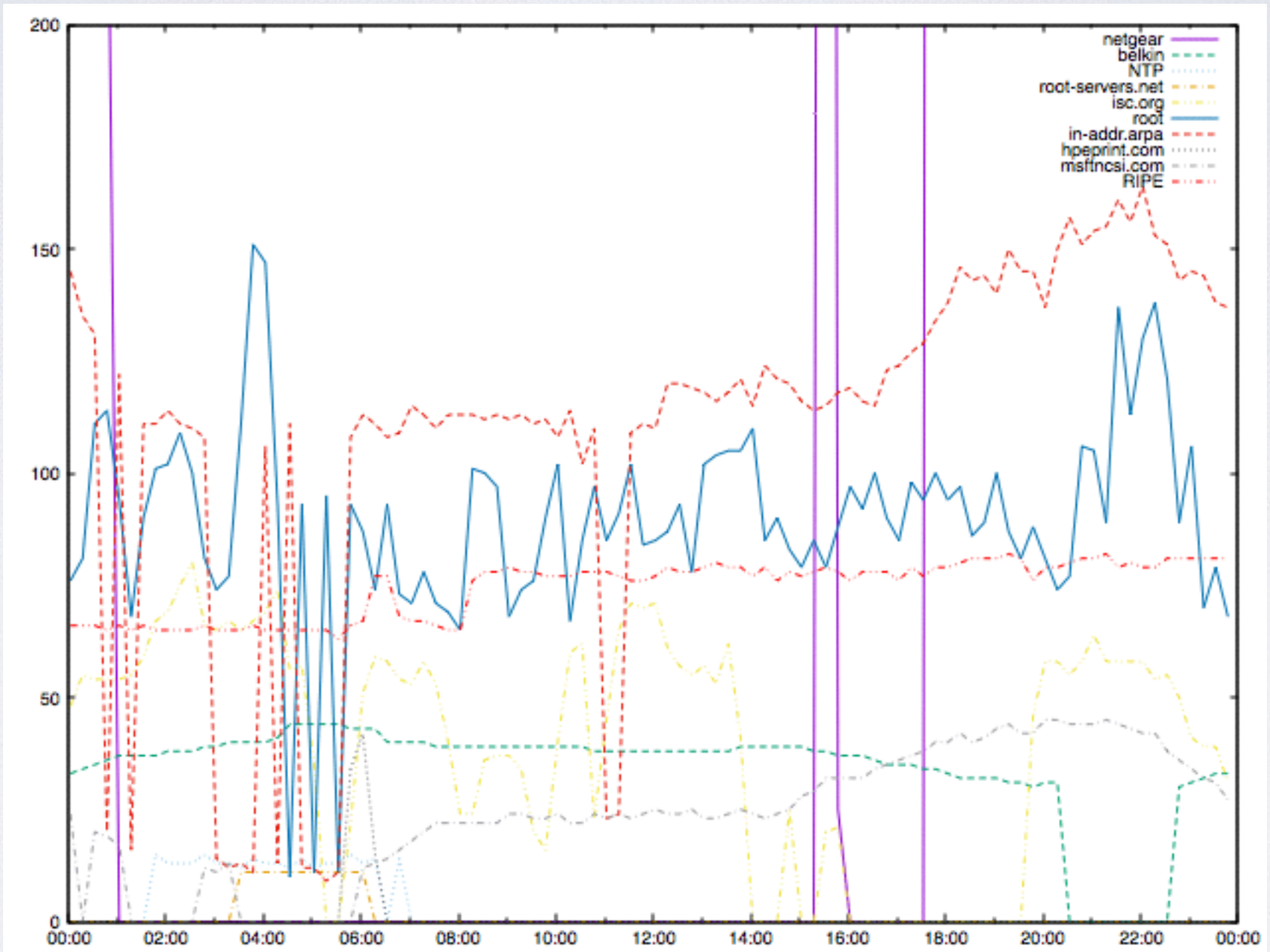
Infrastructure domains



Bond

Internet Systems

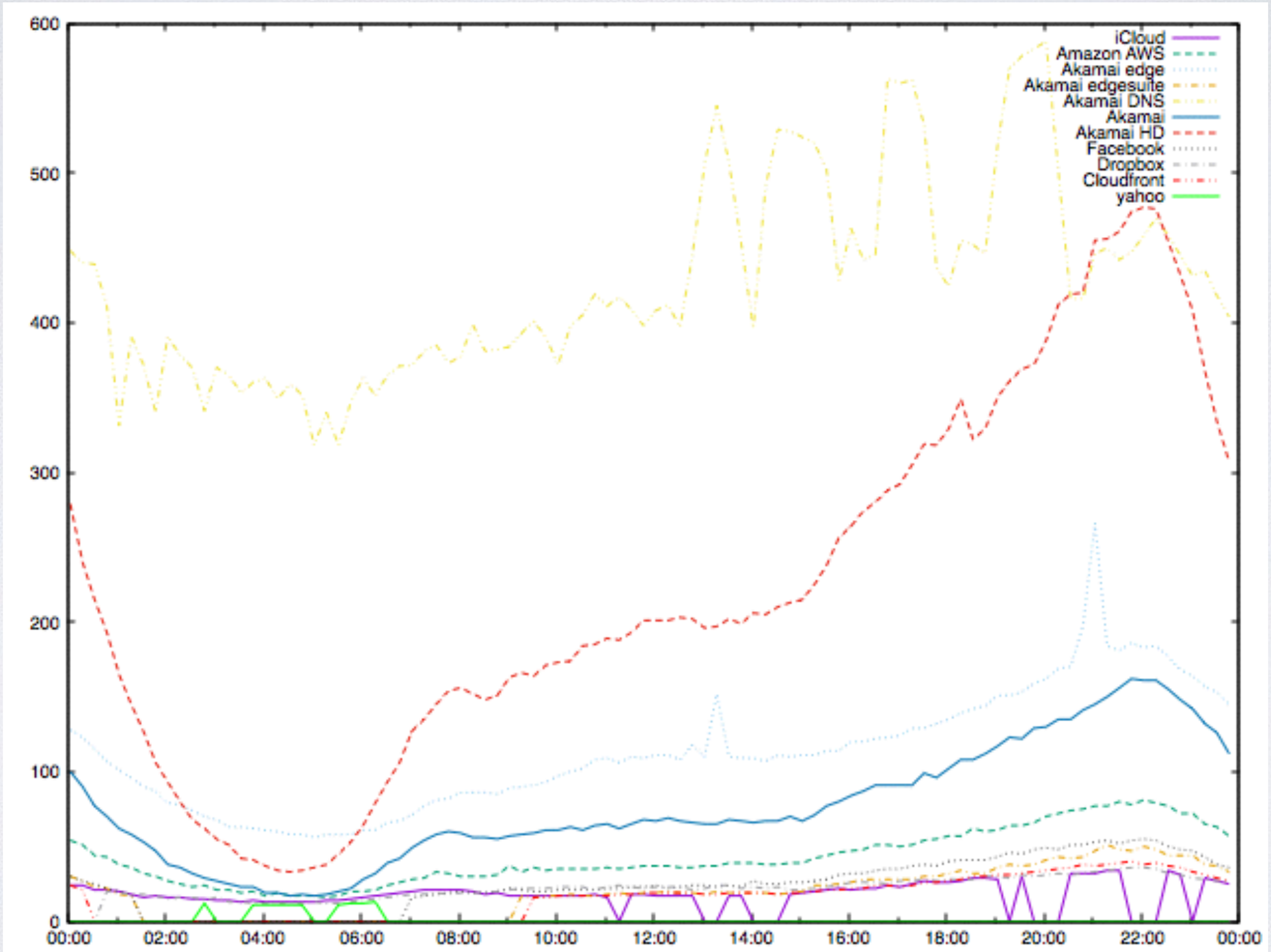
Infrastructure domains zoom



Bond

Internet Systems

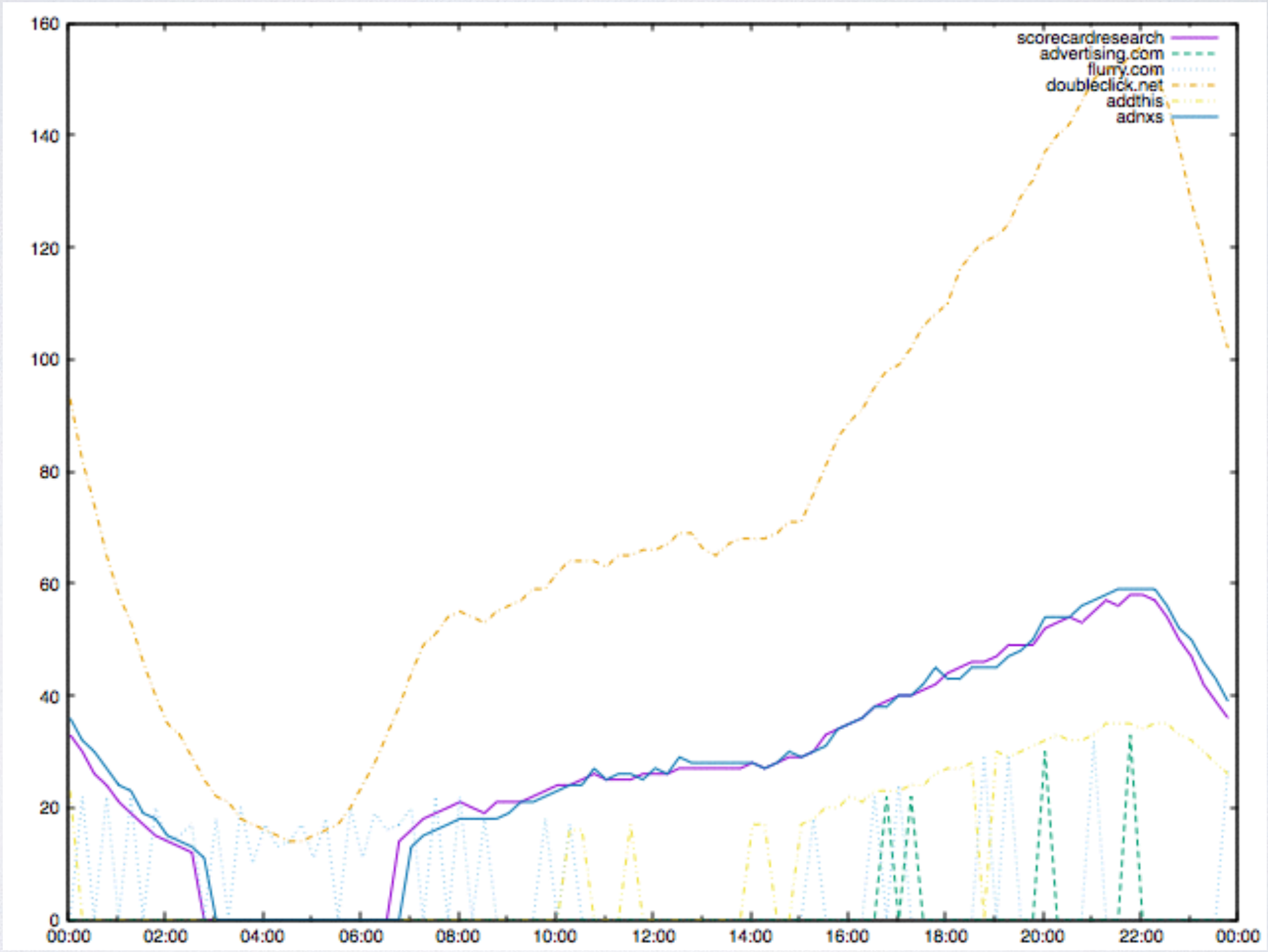
CDNs



Bond

Internet Systems

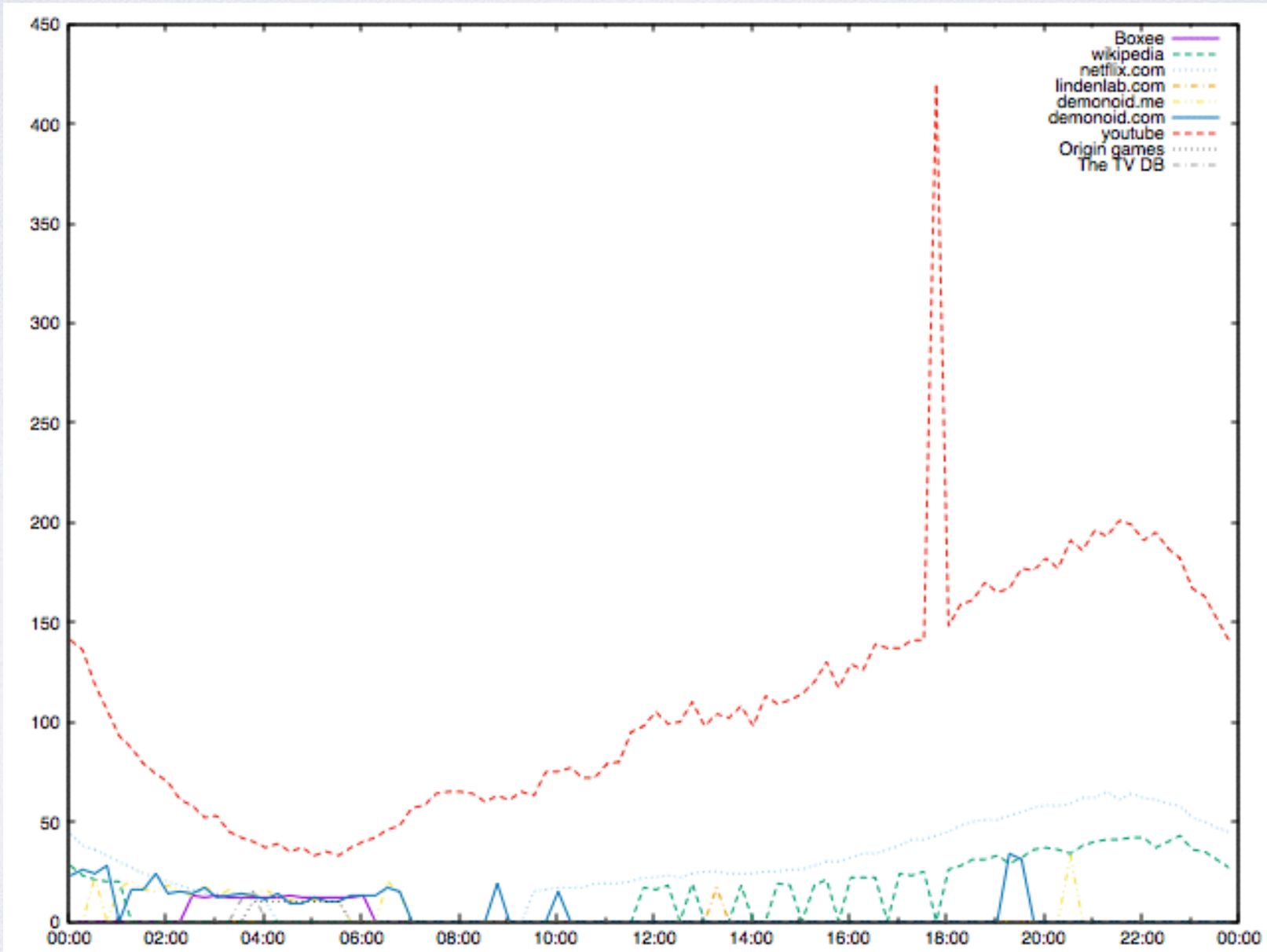
ADs



Bond

Internet Systems

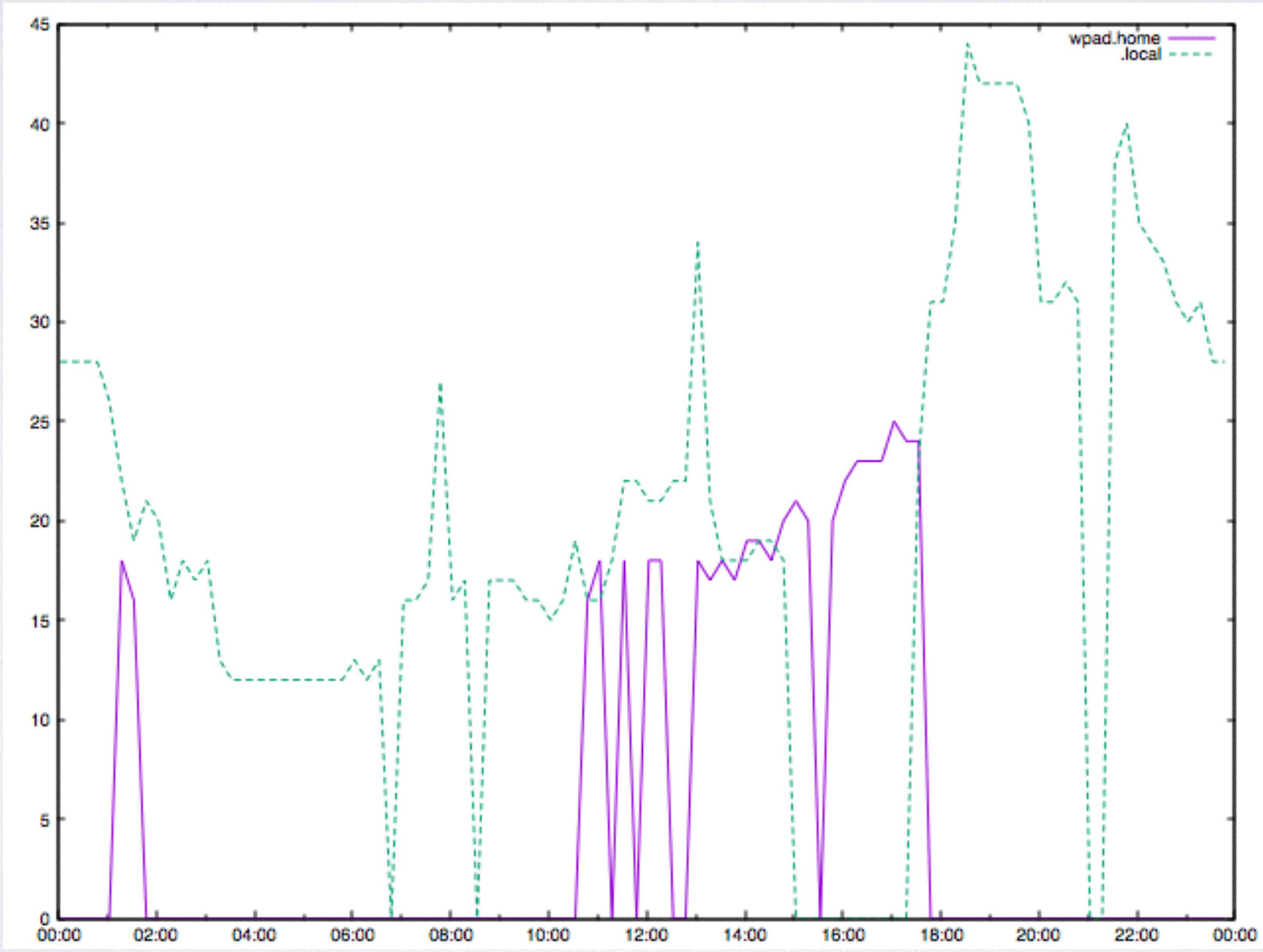
Entertainment sites



Bond

Internet Systems

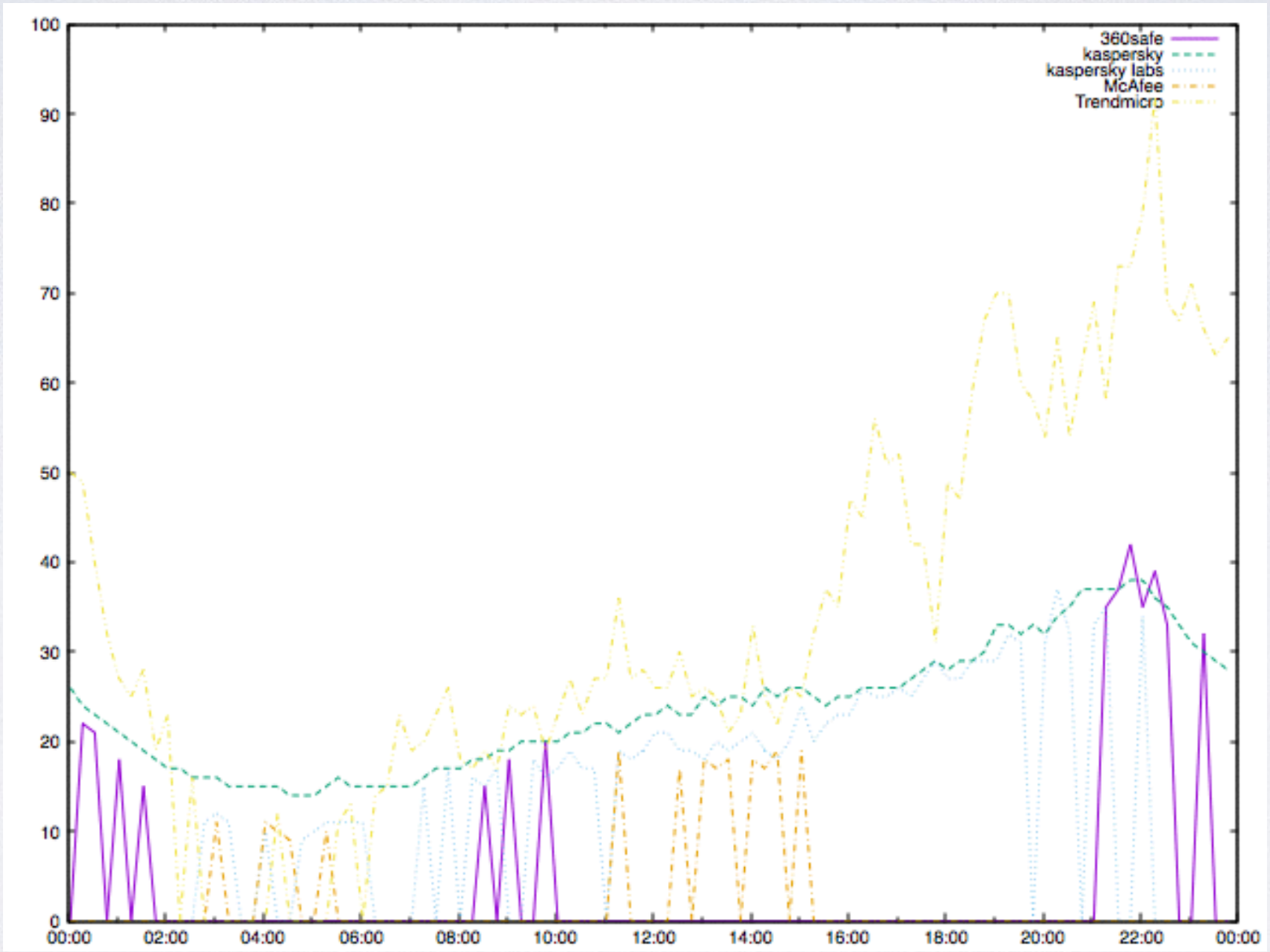
wtf sites



Bond

Internet Systems

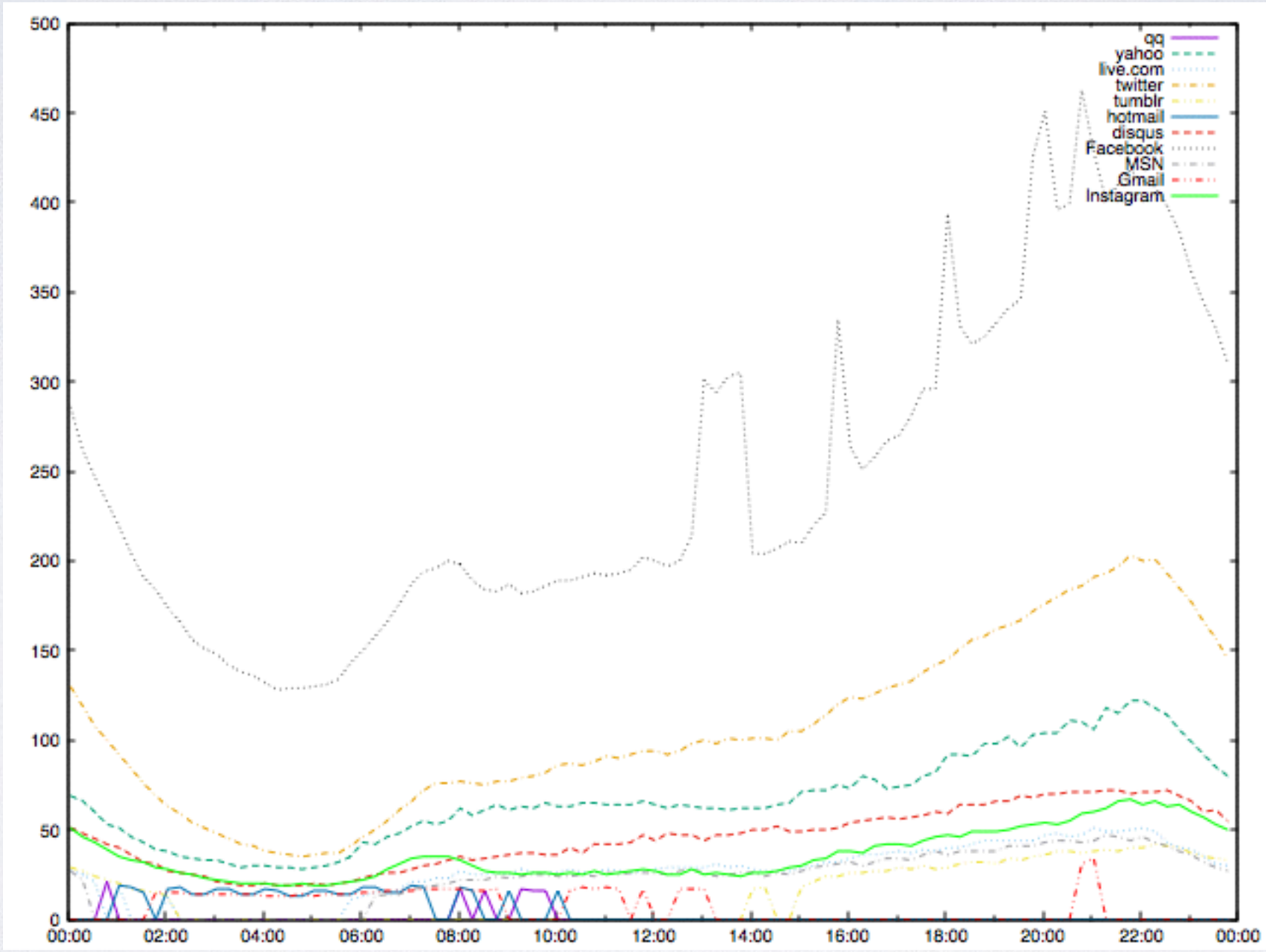
Security services



Bond

Internet Systems

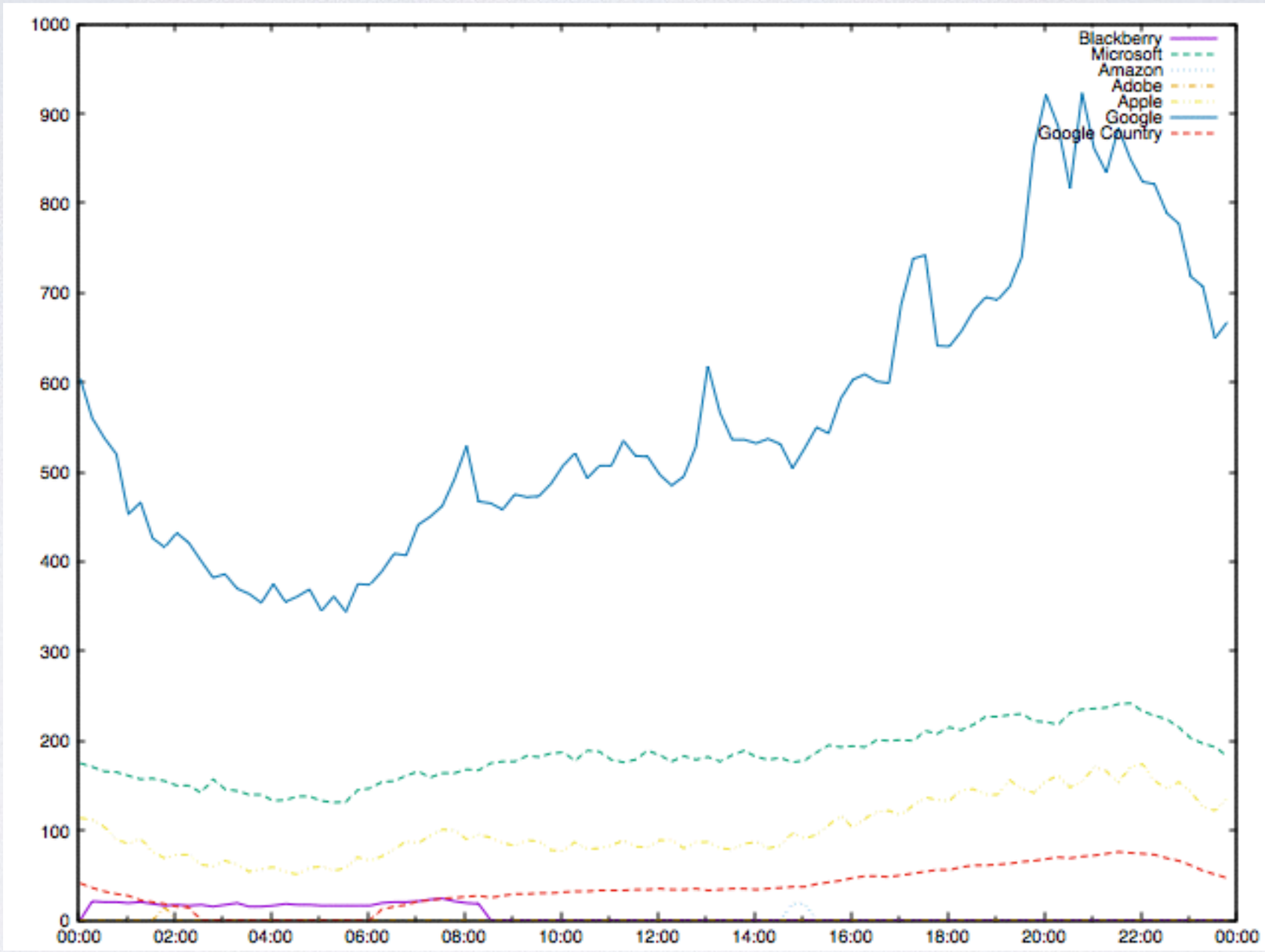
Social



Bond

Internet Systems

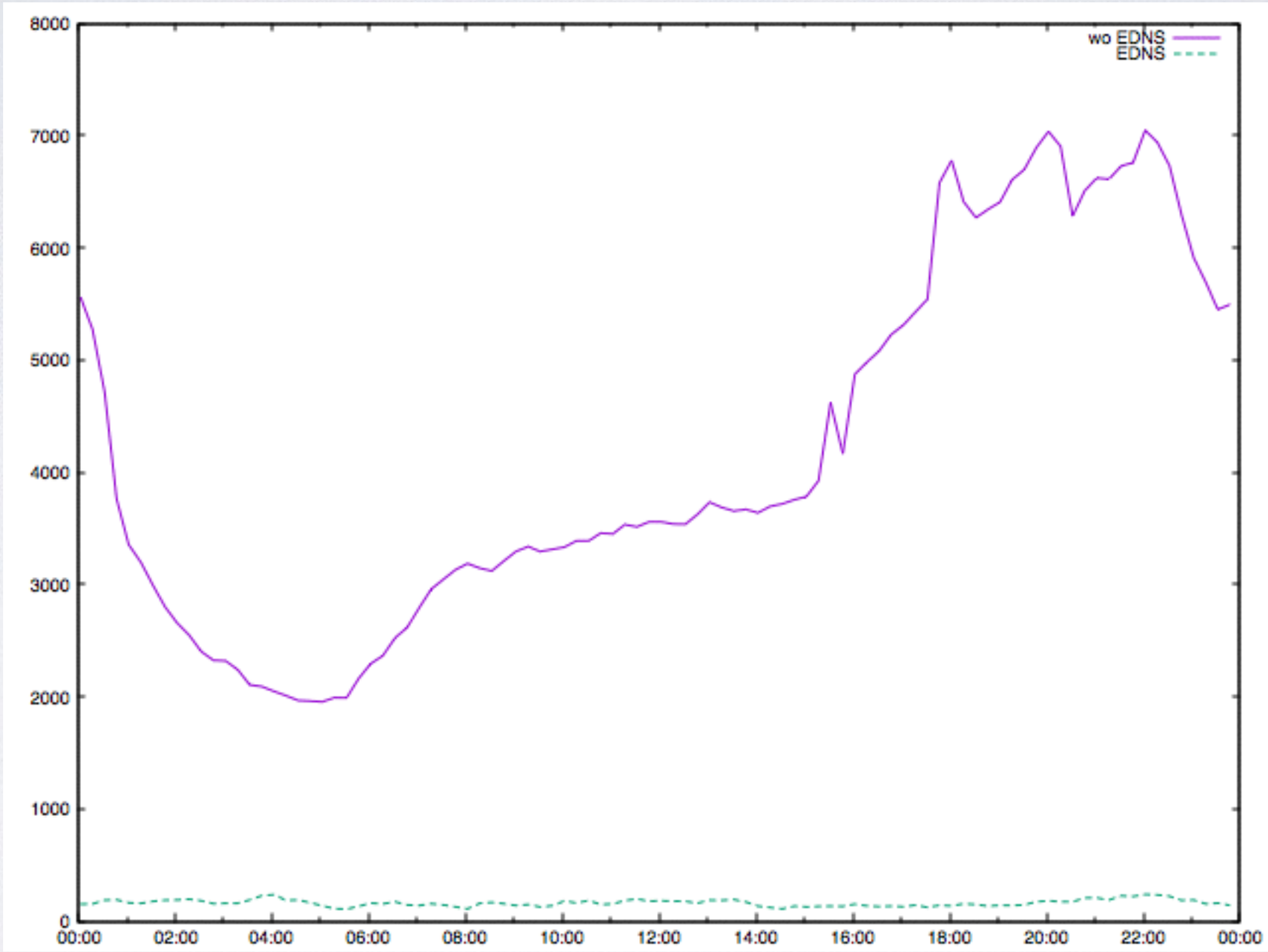
Main domains



Bond

Internet Systems

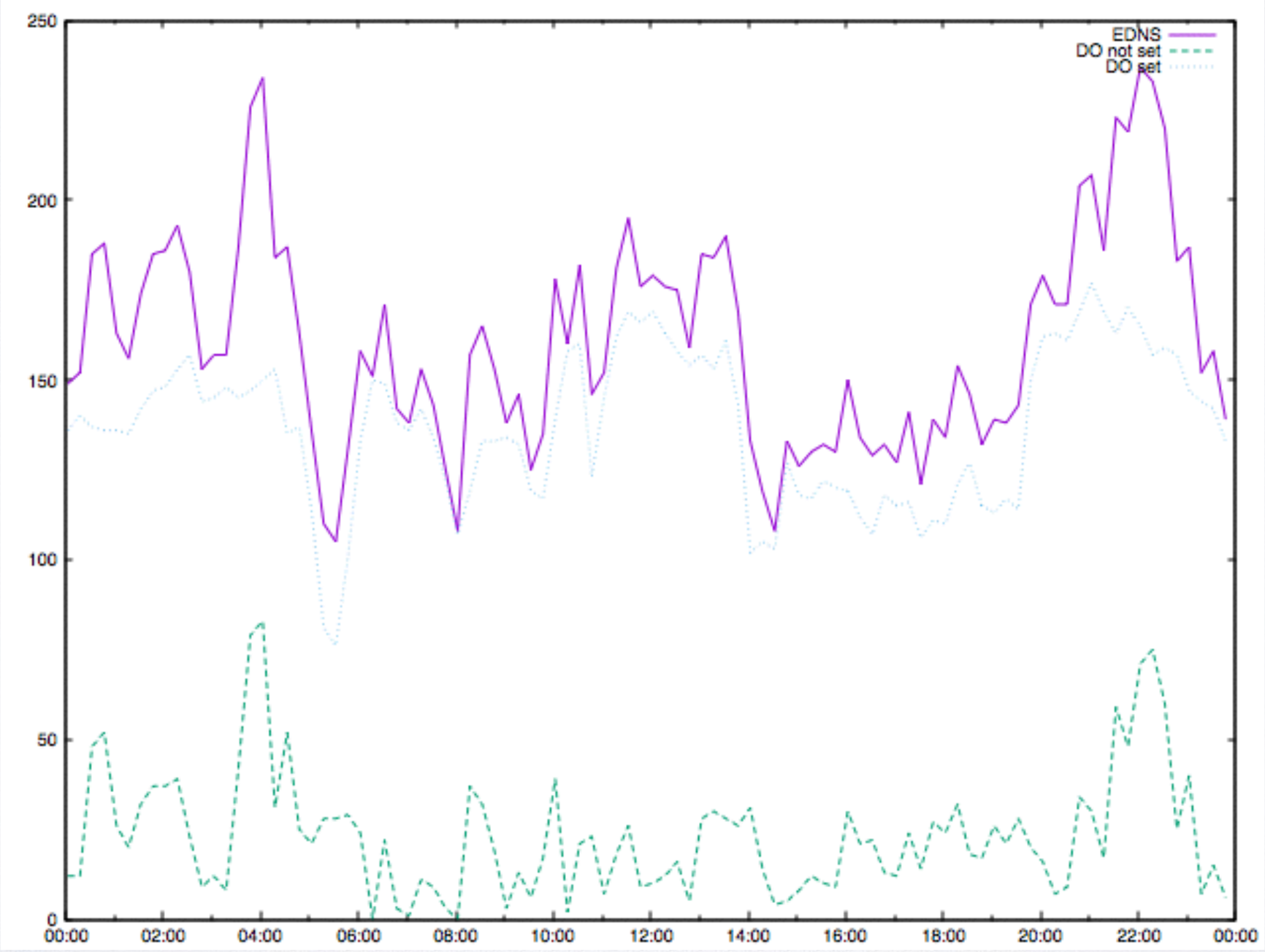
EDNS usage



Bond

Internet Systems

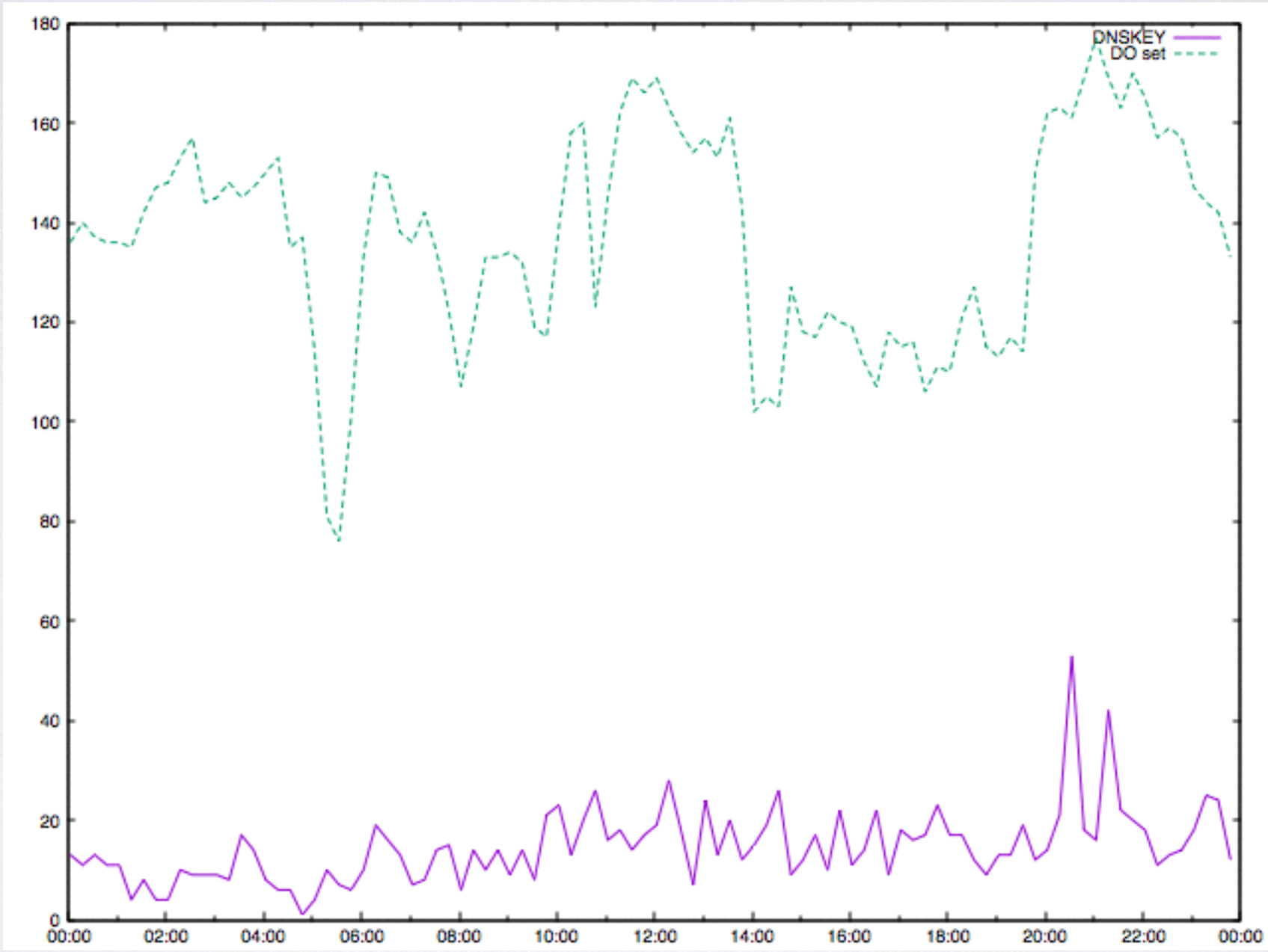
DNSSEC - do



Bond

Internet Systems

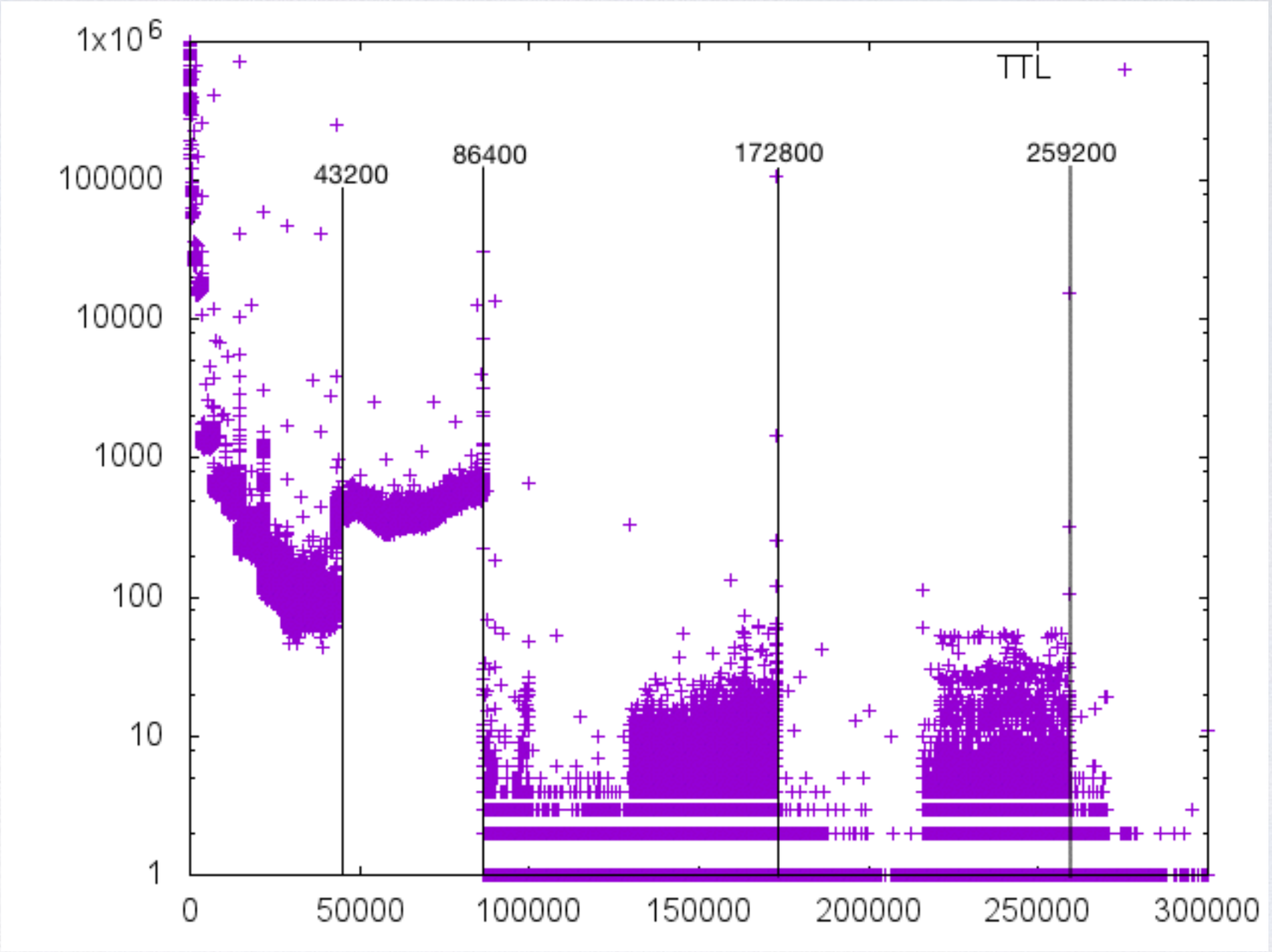
DNSSEC - dnskey



Bond

Internet Systems

TTL



Bond

Internet Systems

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?

Bond

Internet Systems

Acknowledgements

This study was sponsored by a Comcast research grant

Bond

Internet Systems

Questions?