



Always be Effective,
Always be the best

お客様のニーズへ最適な最先端ネットワーク/セキュリティソリューションを

Trafficの可視化

ネットワーク運用の負担軽減について考えてみました

27 Aug 2015

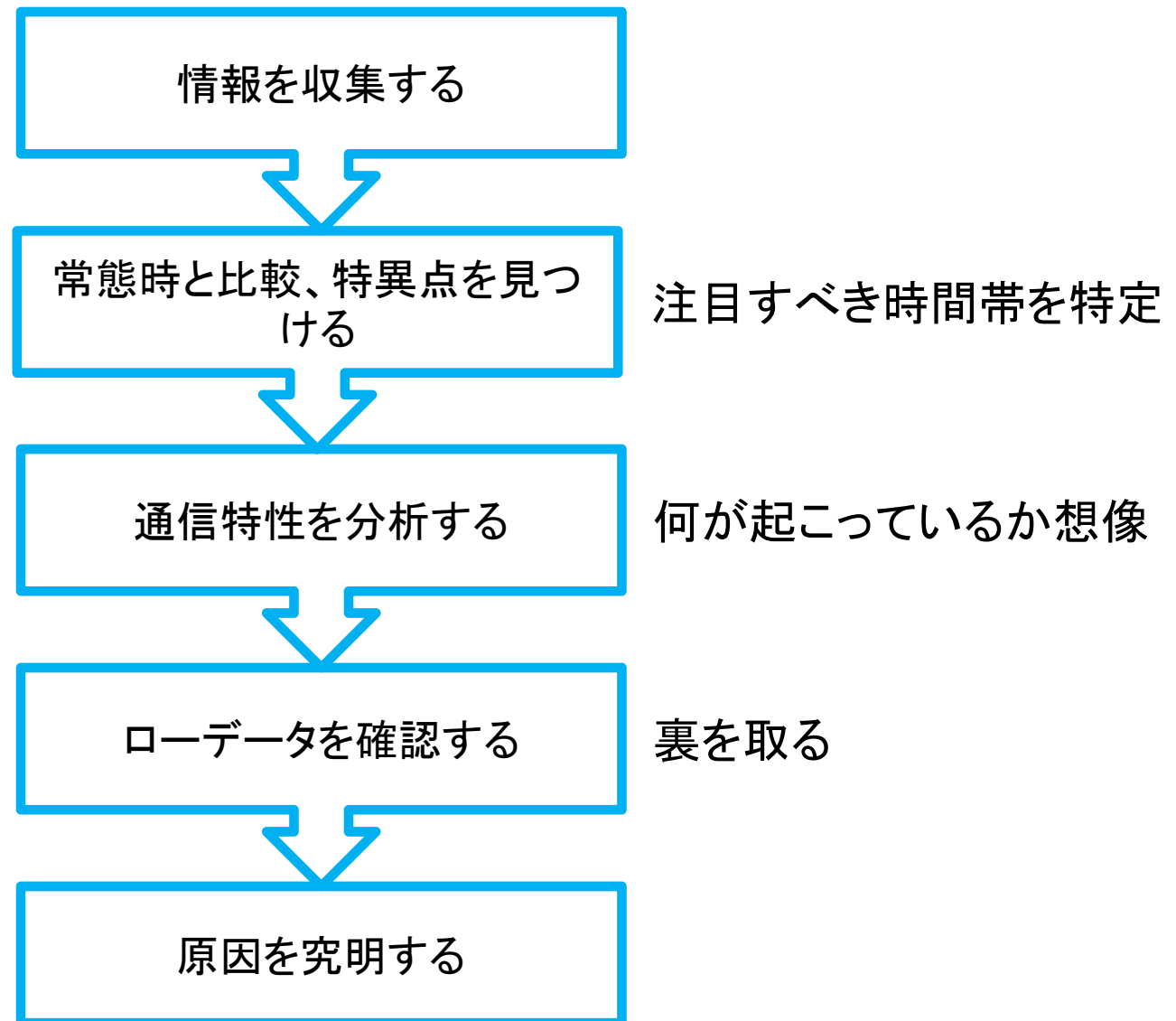
komoriya@terilogy.com

1. 普段の取り組み(かもしれないこと)

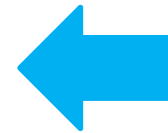
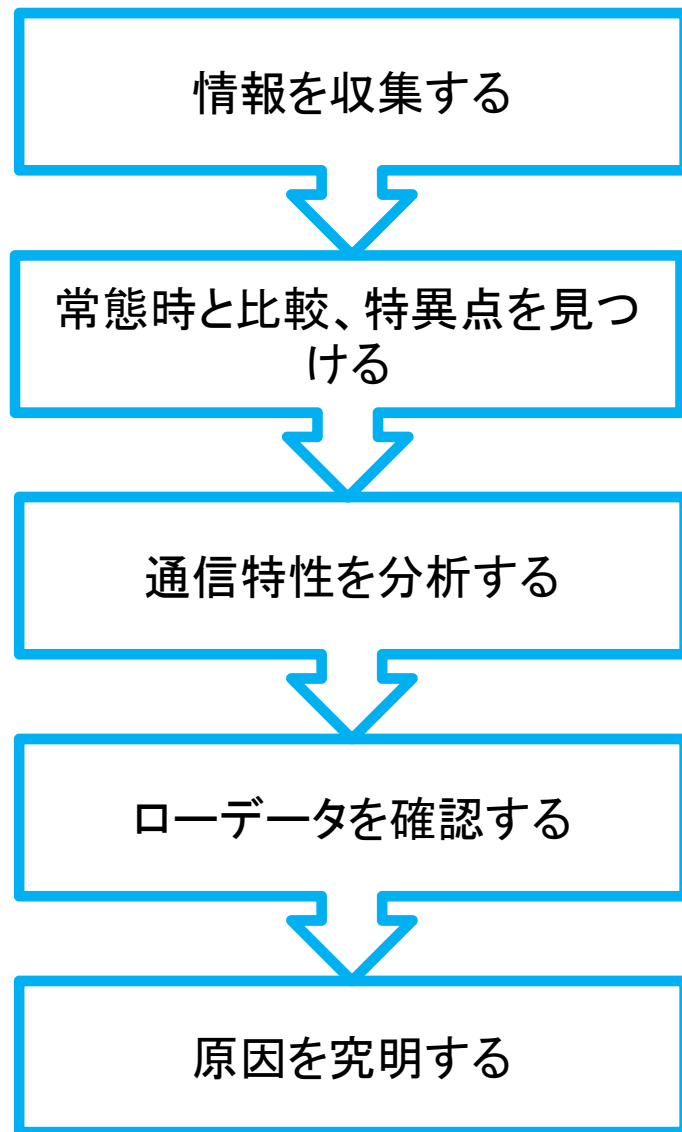
普段のネットワーク運用のなかでやっていること:

1. 速やかに、インシデントに気づく
2. 速やかに、起こっている内容について理解する
3. 速やかに、対策を実施する

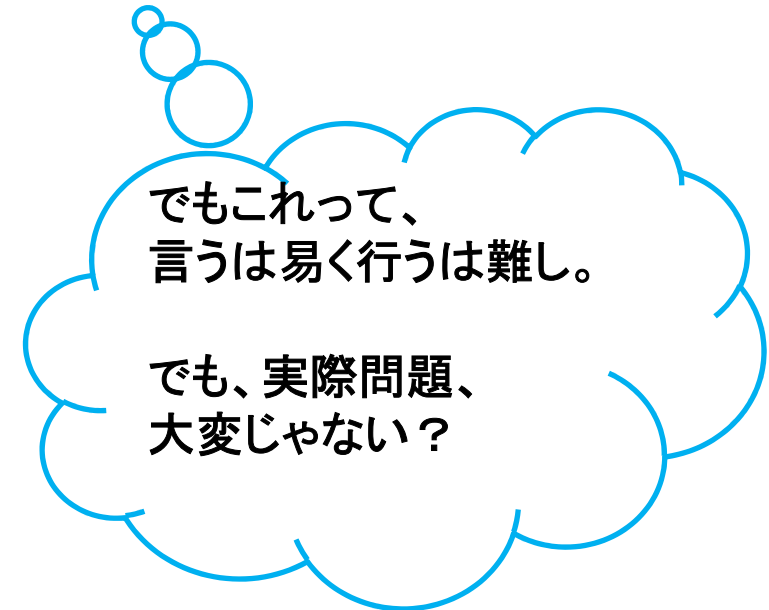
2. 調査のフロー



2. 調査のフロー



この流れで動けばいいける！



NetFlowとかで中身がわかると思えないし

pcapなんてデカすぎて見きれないし

どうする、オレ

3. なんか道具が欲しい

- DNSサーバの運用を考えつつ、こんな風にできるといいのかも、の例

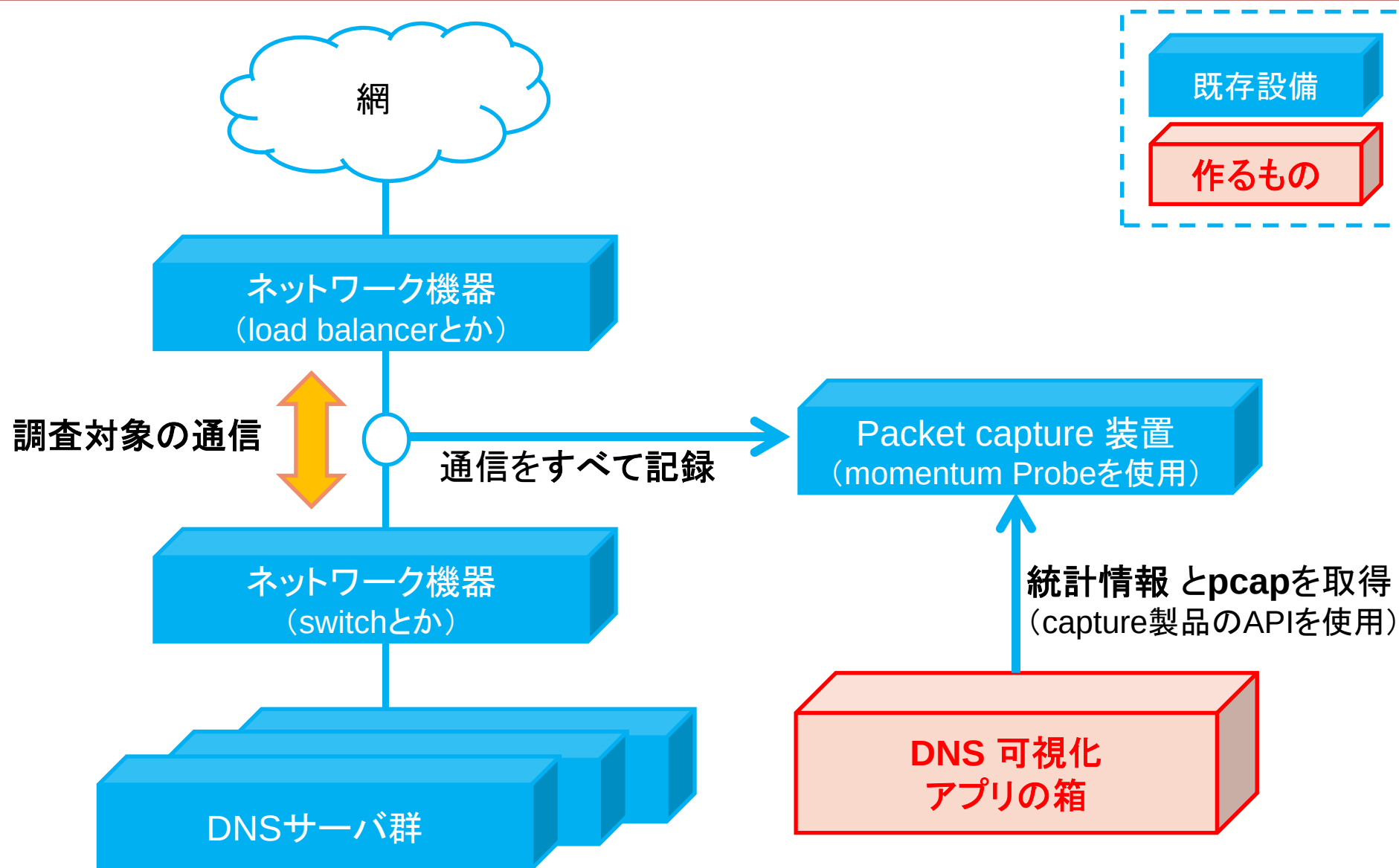


3. なんか道具が欲しい

- DNSサーバの運用を考えつつ作ってみる道具の範囲



4. 利用環境



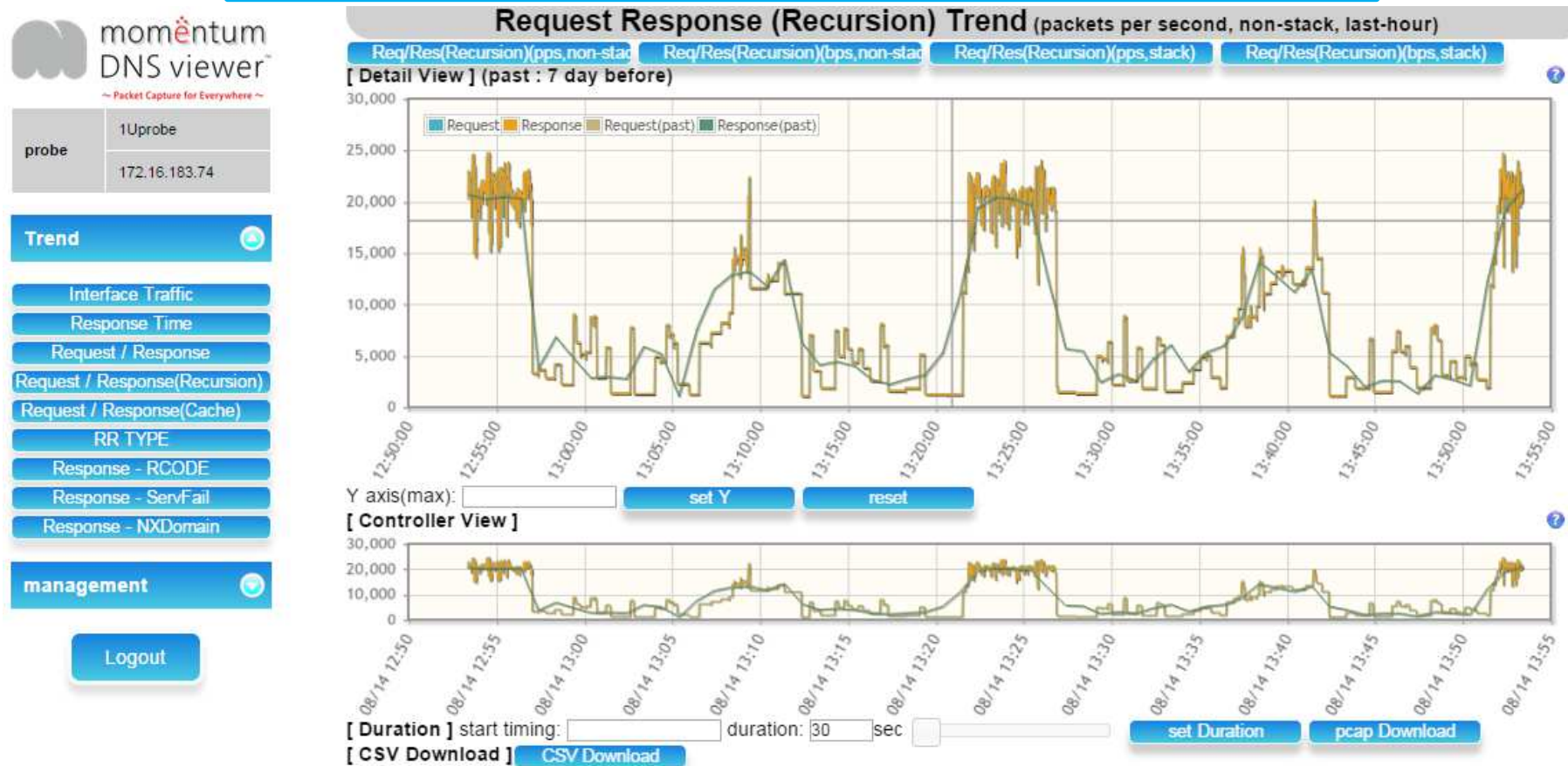
5. 作ってみました

ユーザ登録 : 必要
利用 : 無償でOK

仮説 : 「これまでよりも細かく可視化できる道具があれば、
運用の大変さがかわるかもしれない」

作ったもの: DNS viewer

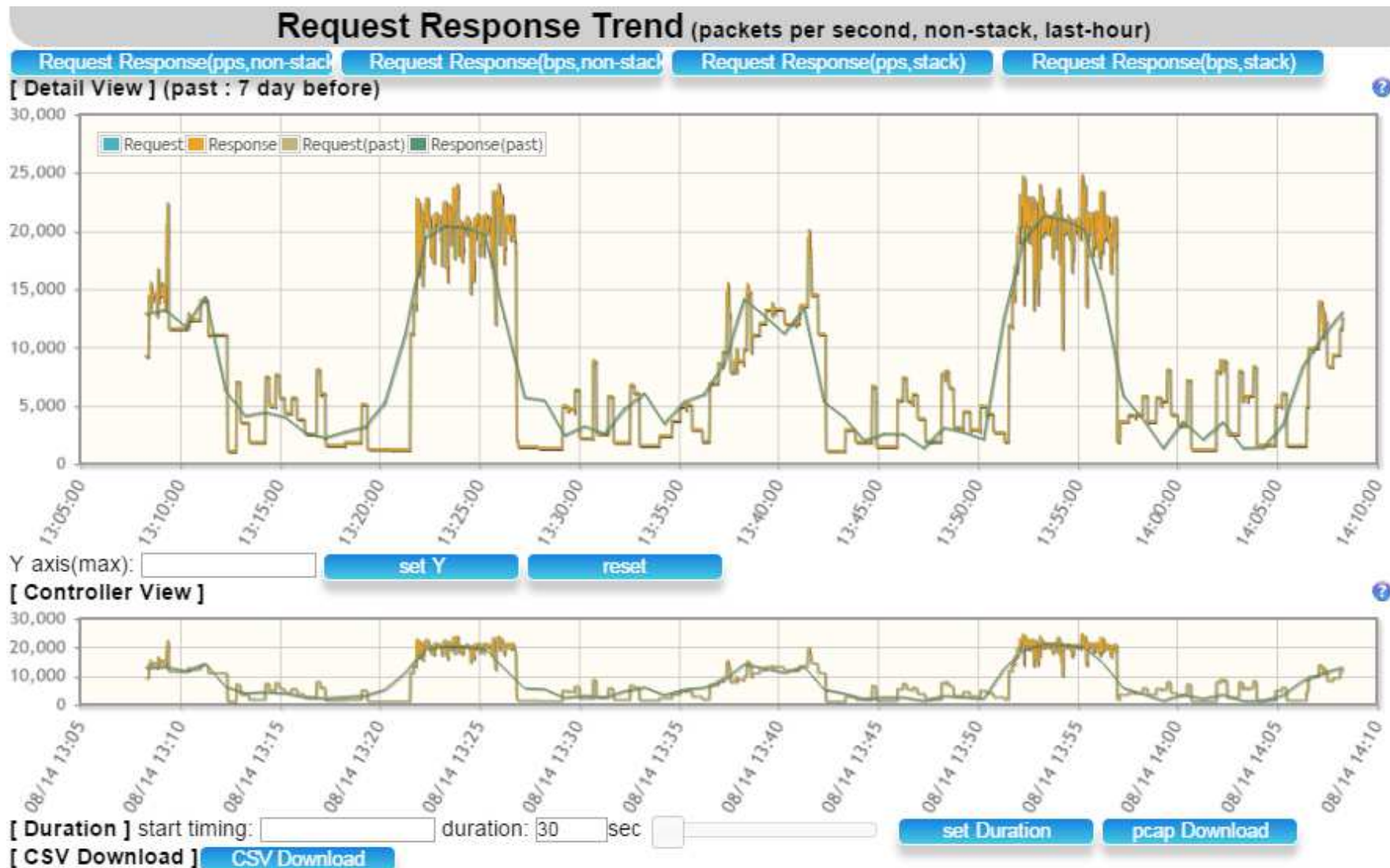
公開場所 : http://tapas.terilogy.com/projects/dns_viewer



6. できるようになったこと

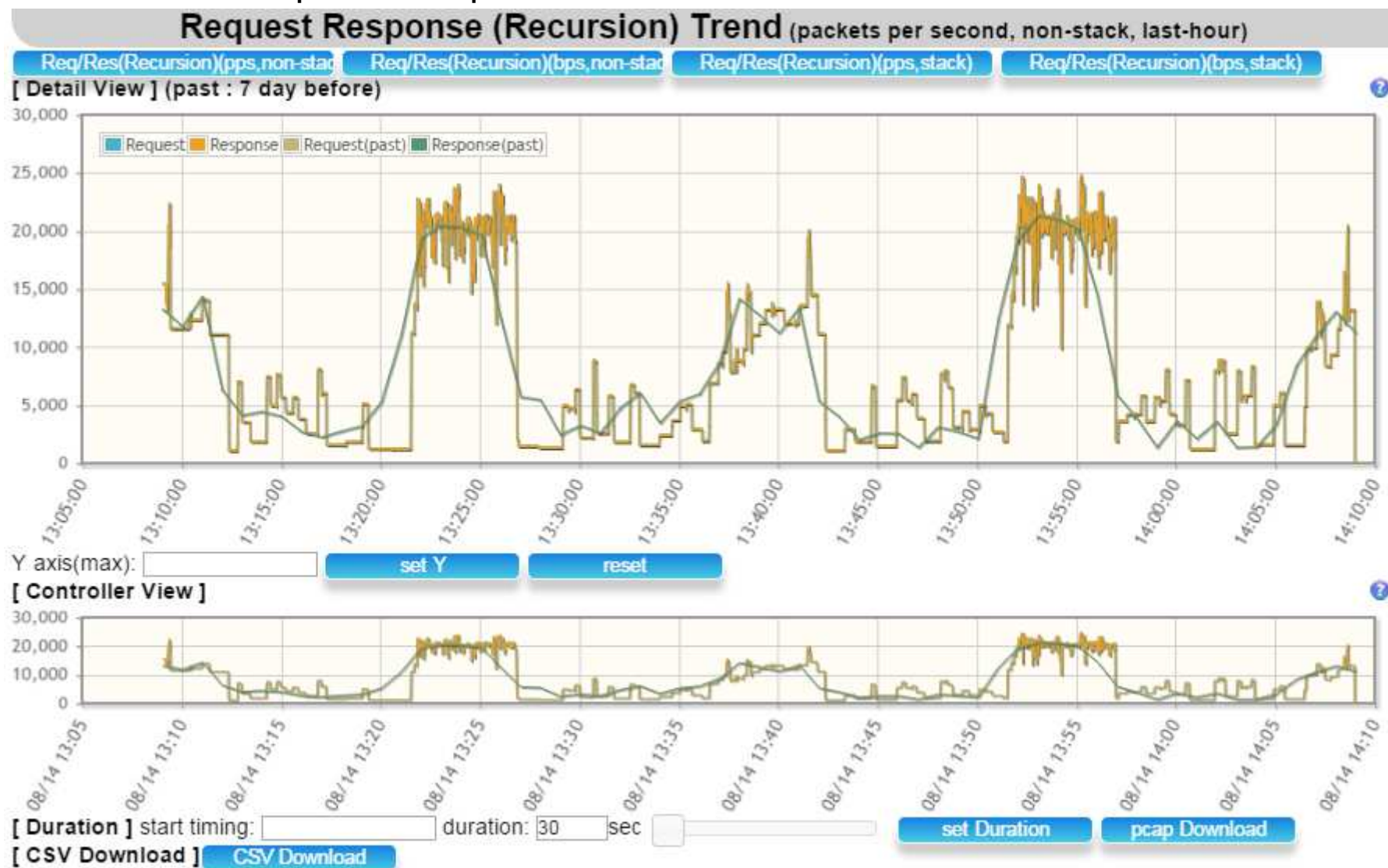
先週より多いな、とか。

DNSのRequestとResponseが見えました(過去情報も表示)(pps、bpsとかを1秒粒度で)



6. できるようになったこと

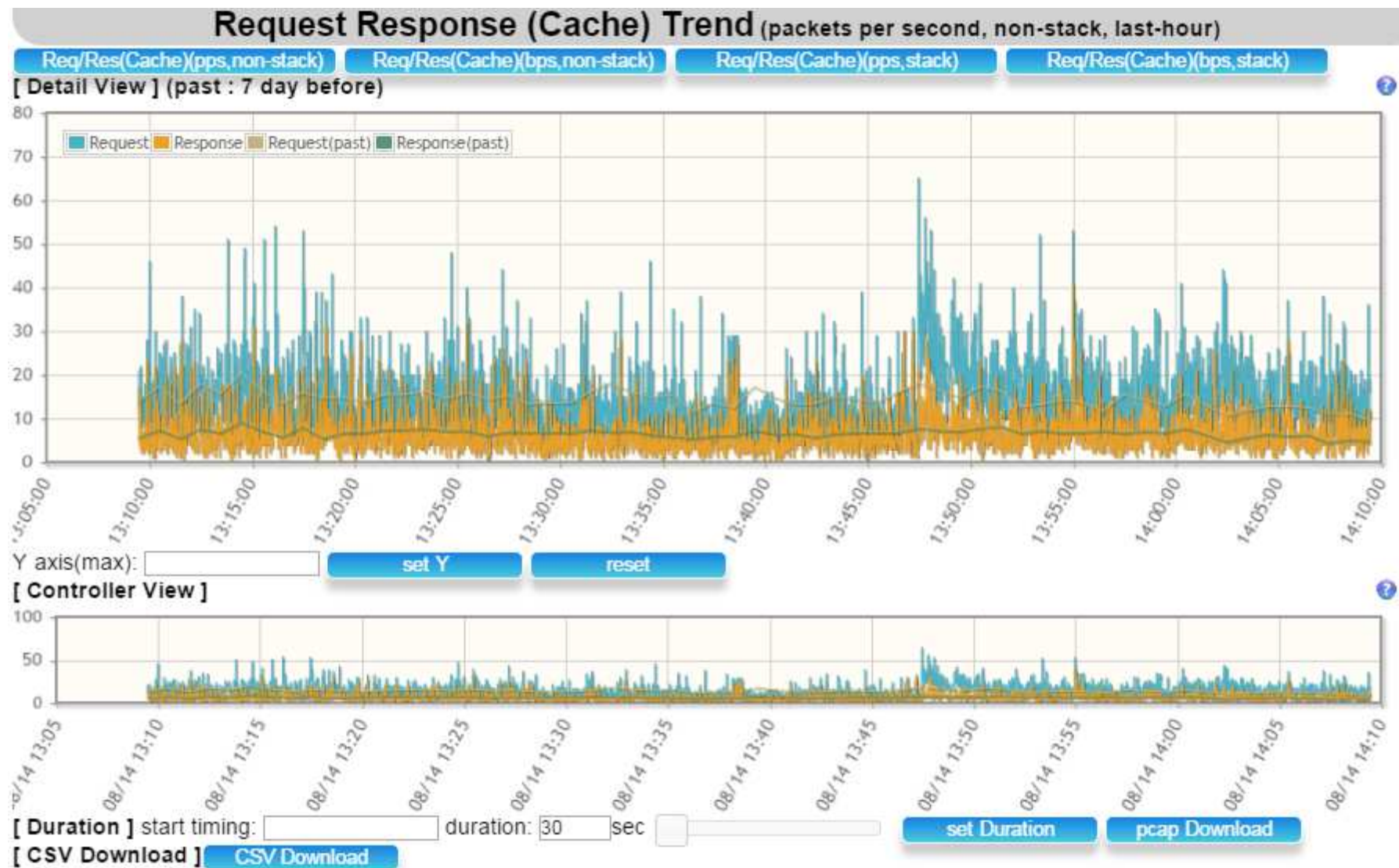
DNSのRequestとResponseが見えました(Recursion Desiredのみを表示)



6. できるようになったこと

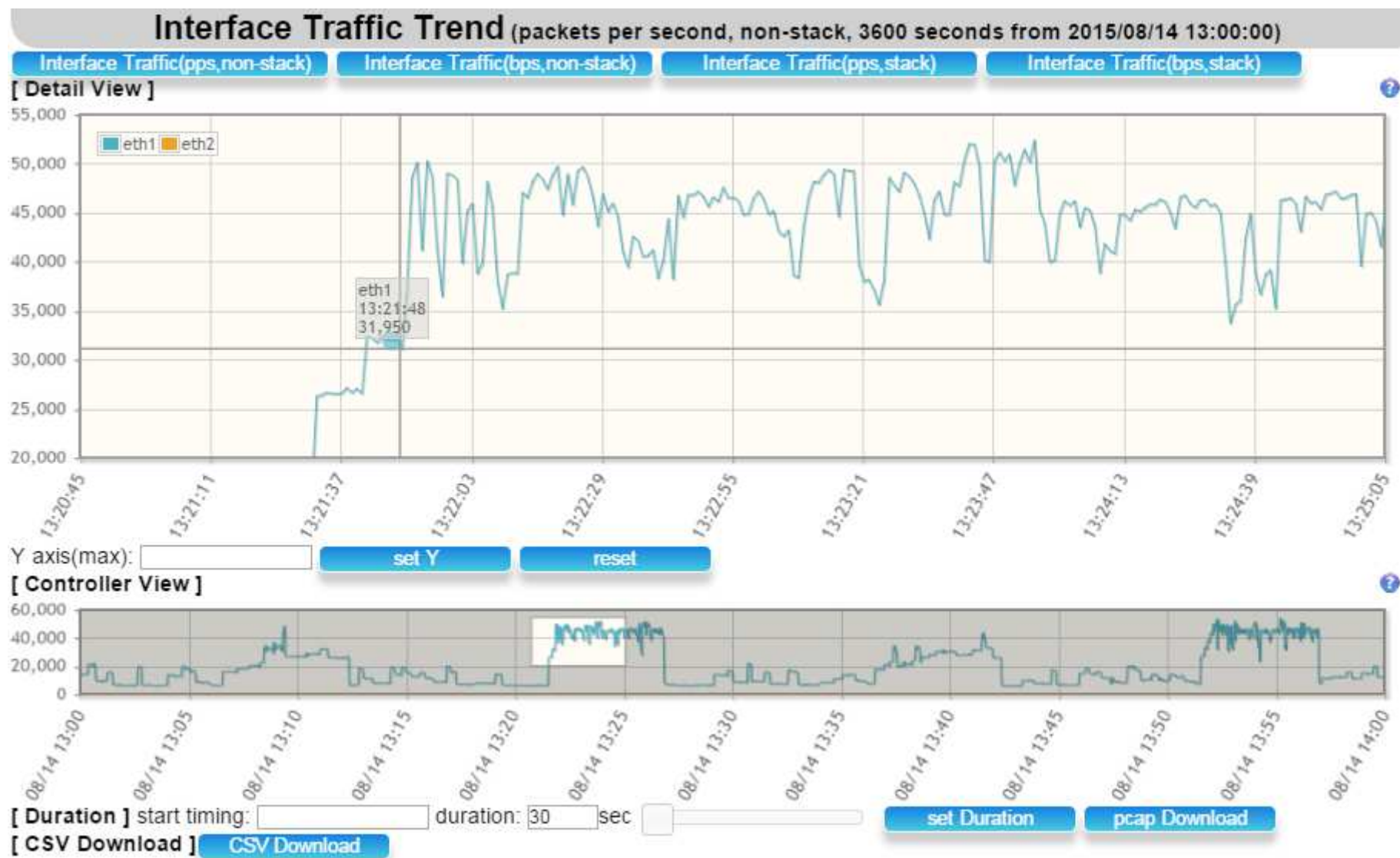
Cache missした結果の通信が見える

DNSのRequestとResponseが見えました(Cache Serverの通信のみを表示)



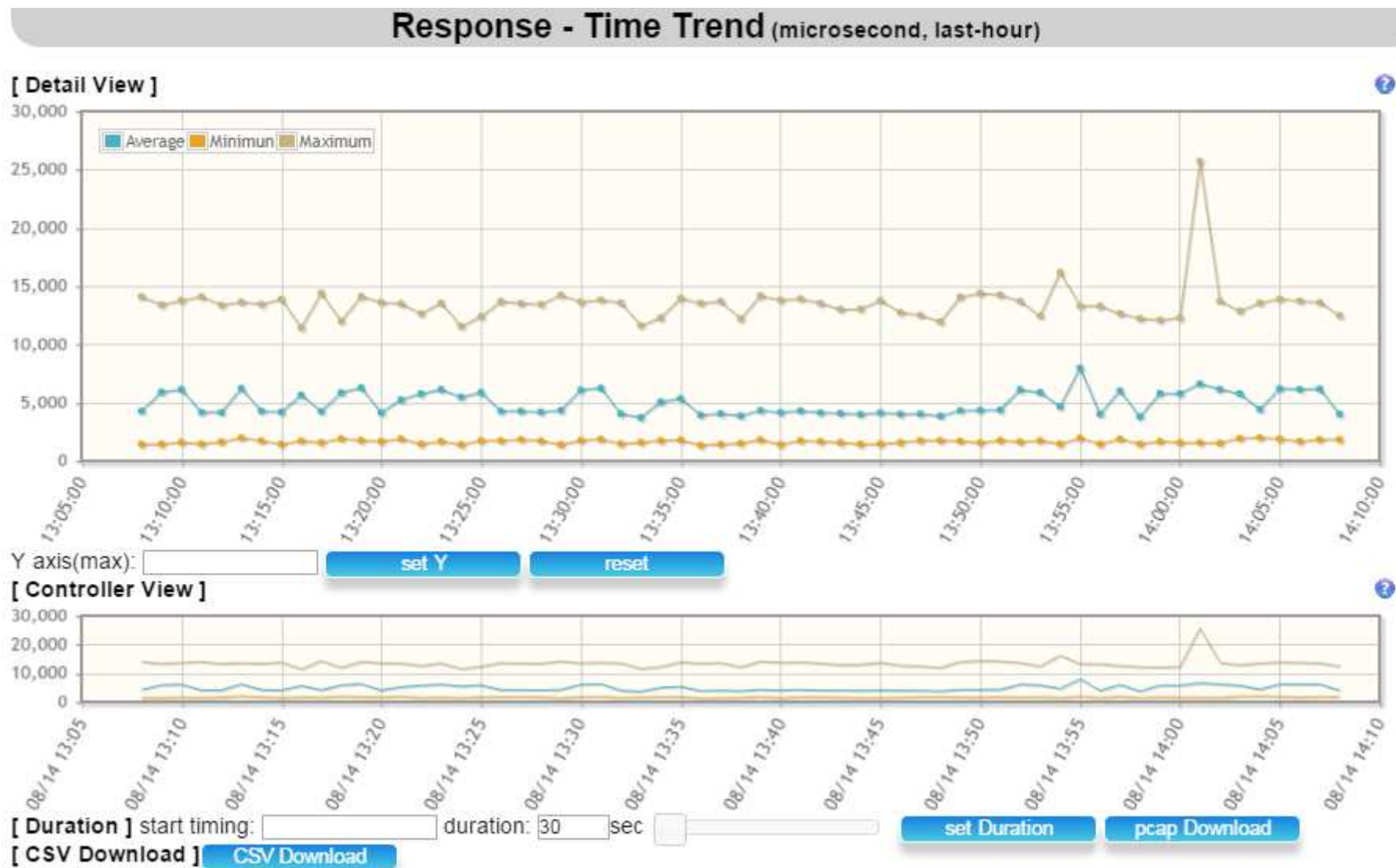
6. できるようになったこと

拡大して見るできるようになりました



6. できるようになったこと

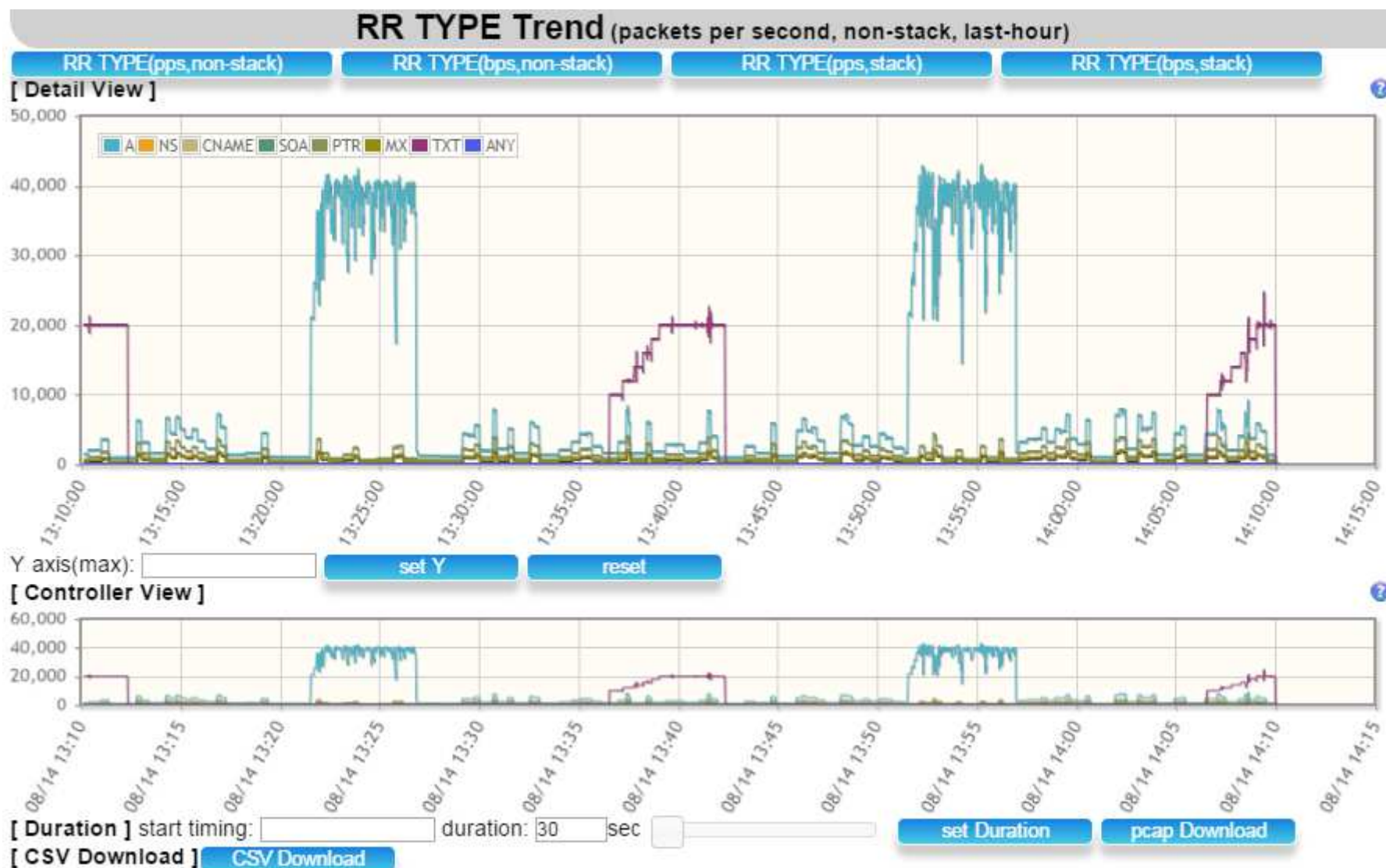
DNSサーバの応答時間見えました(ここだけ、アクティブ検査)



6. できるようになったこと

TXTとかANYとか増えたら嫌です

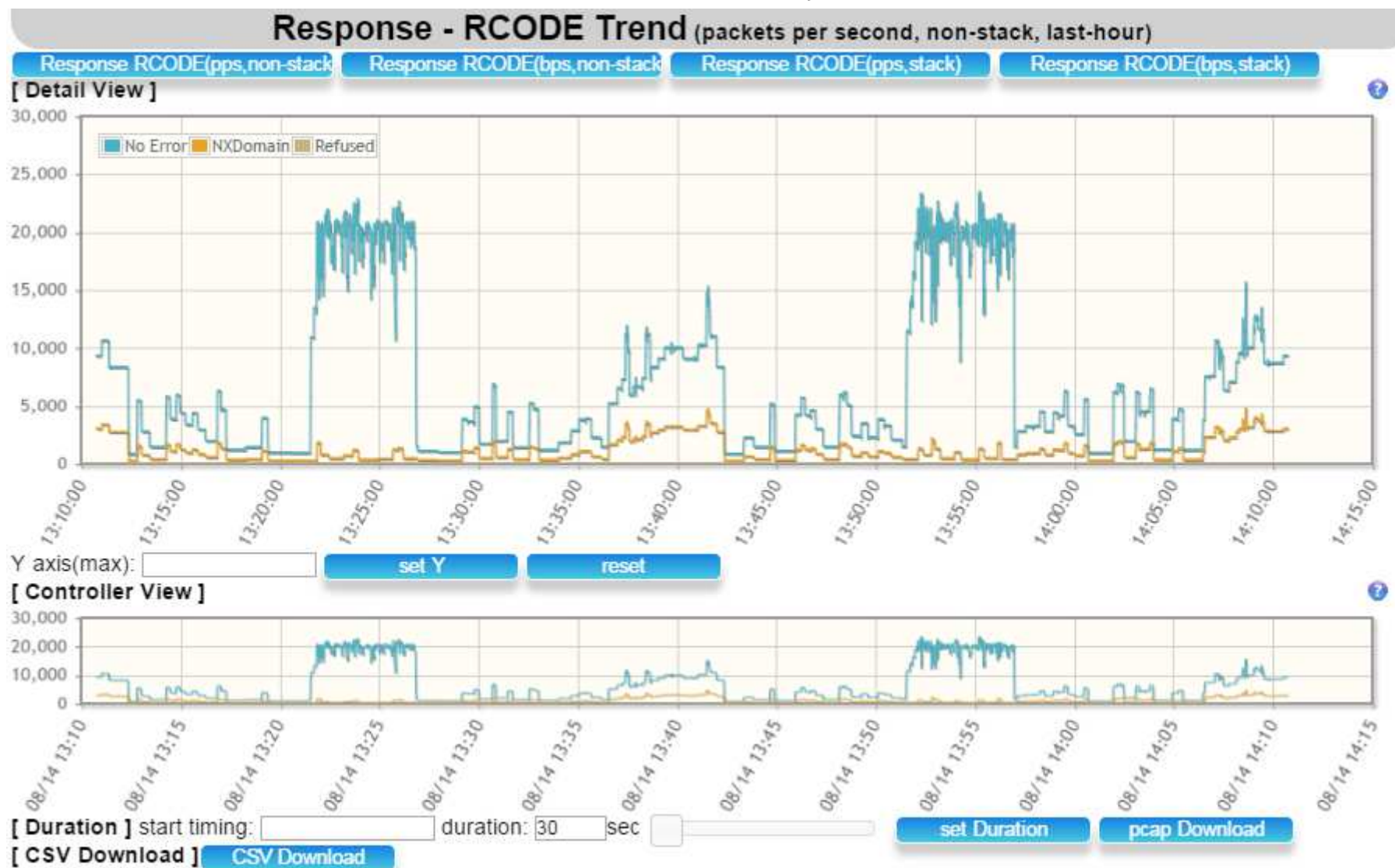
DNSのRRの配合が見えました



6. できるようになったこと

NXDomainとか増えたら嫌です

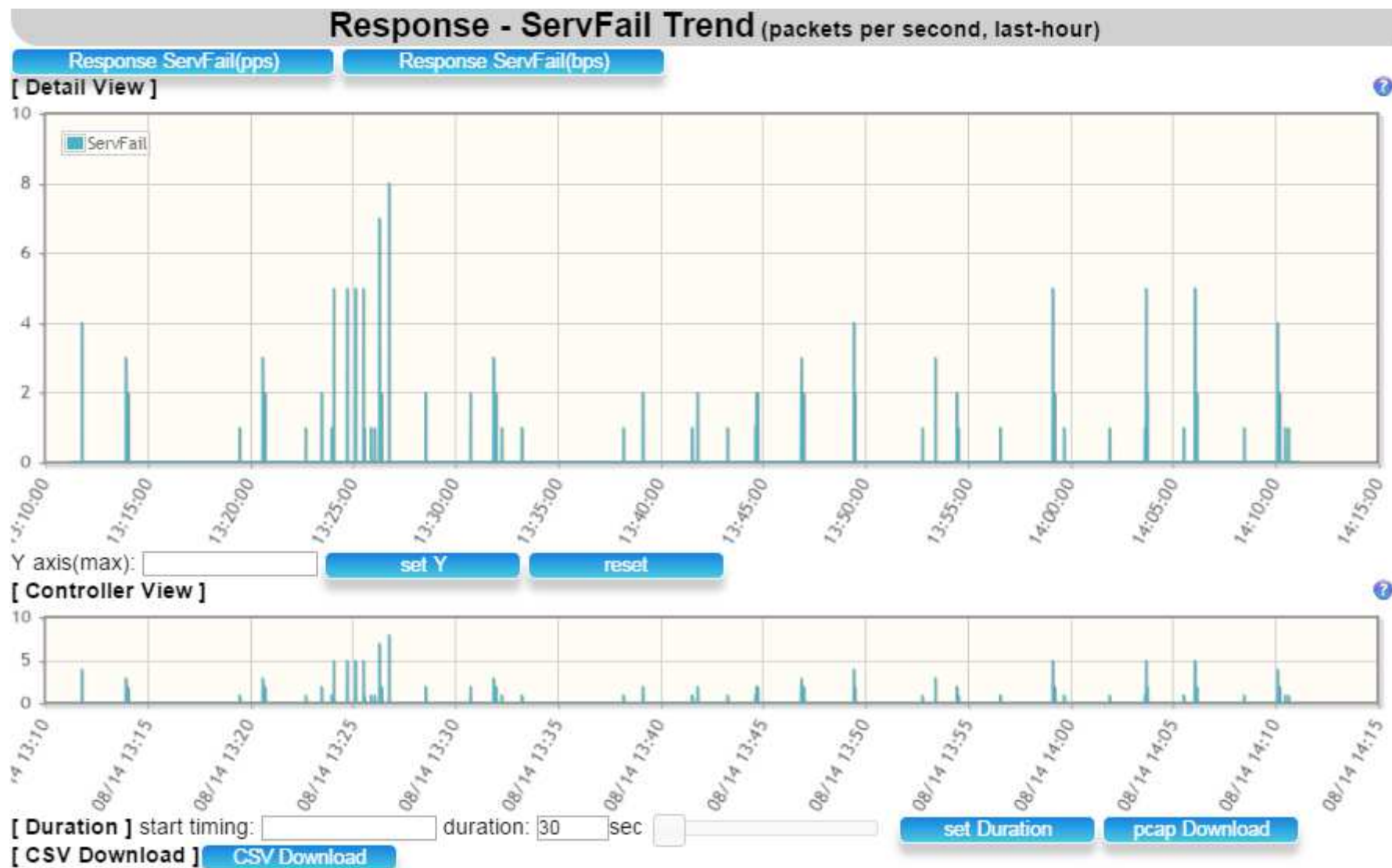
DNSのRCODEの配合が見えました



6. できるようになったこと

ServFailとかあったら嫌です

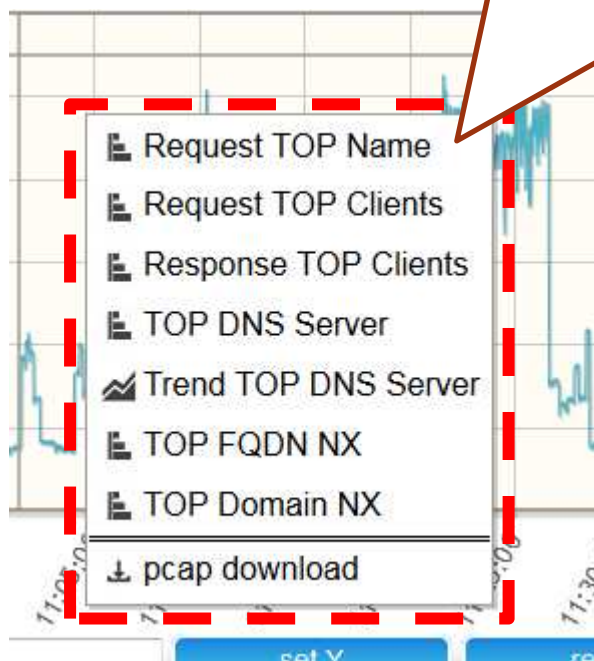
DNSのServFailが見えました



6. できるようになったこと

各種Trend画面から、いくつかの切り口でTOPランクが見えます

Trend画面で見ている任意の時間幅に対して
いくつかの切り口でTOPランクを確認できる



6. できるようになったこと

直前の時間帯からの増加率も見える

DNSの検索されてるFQDNが見えました

Request - TOP10 Name (custom:2015/08/14 13:35:56 ~ 2015/08/14 13:37:58 : 122 sec)

[Graph View]



[pcap Download Condition]

[pcap Download] start timing: 2015/08/14 13:35:56 duration: 122 sec

Download

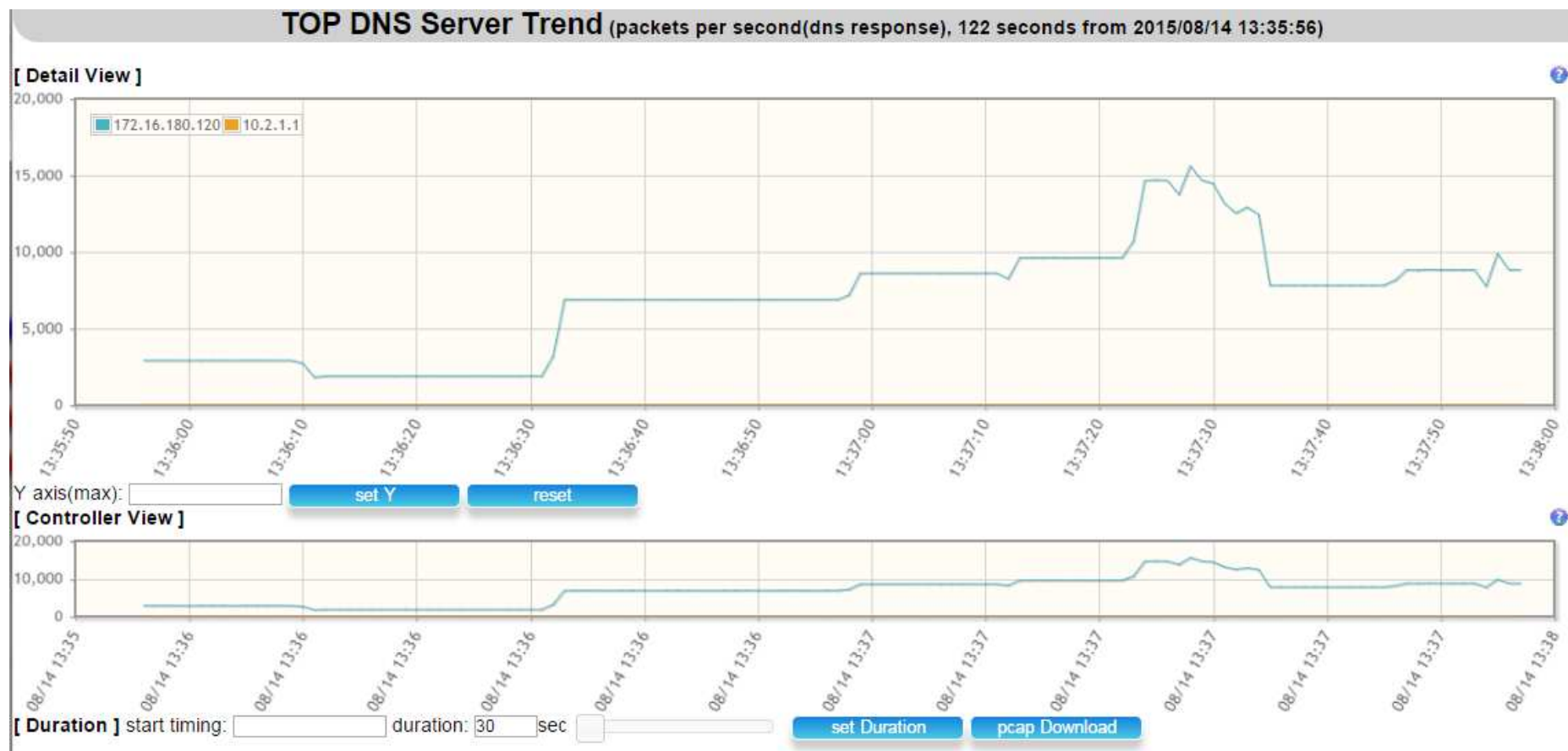
[Comparative Table]

#	FQDN	# of Query(current term)	# of Query(previous term)	rate of change
1	aaa.test.com	120,567	0	-
2	bbb.test.com	120,567	0	-
3	ccc.test.com	120,567	0	-
4	web.test.com	120,566	0	-
5	terilogy.com	78,992	92,716	85 %
6	11 1 168 192 in-addr arpa	39 496	46 358	85 %

6. できるようになったこと

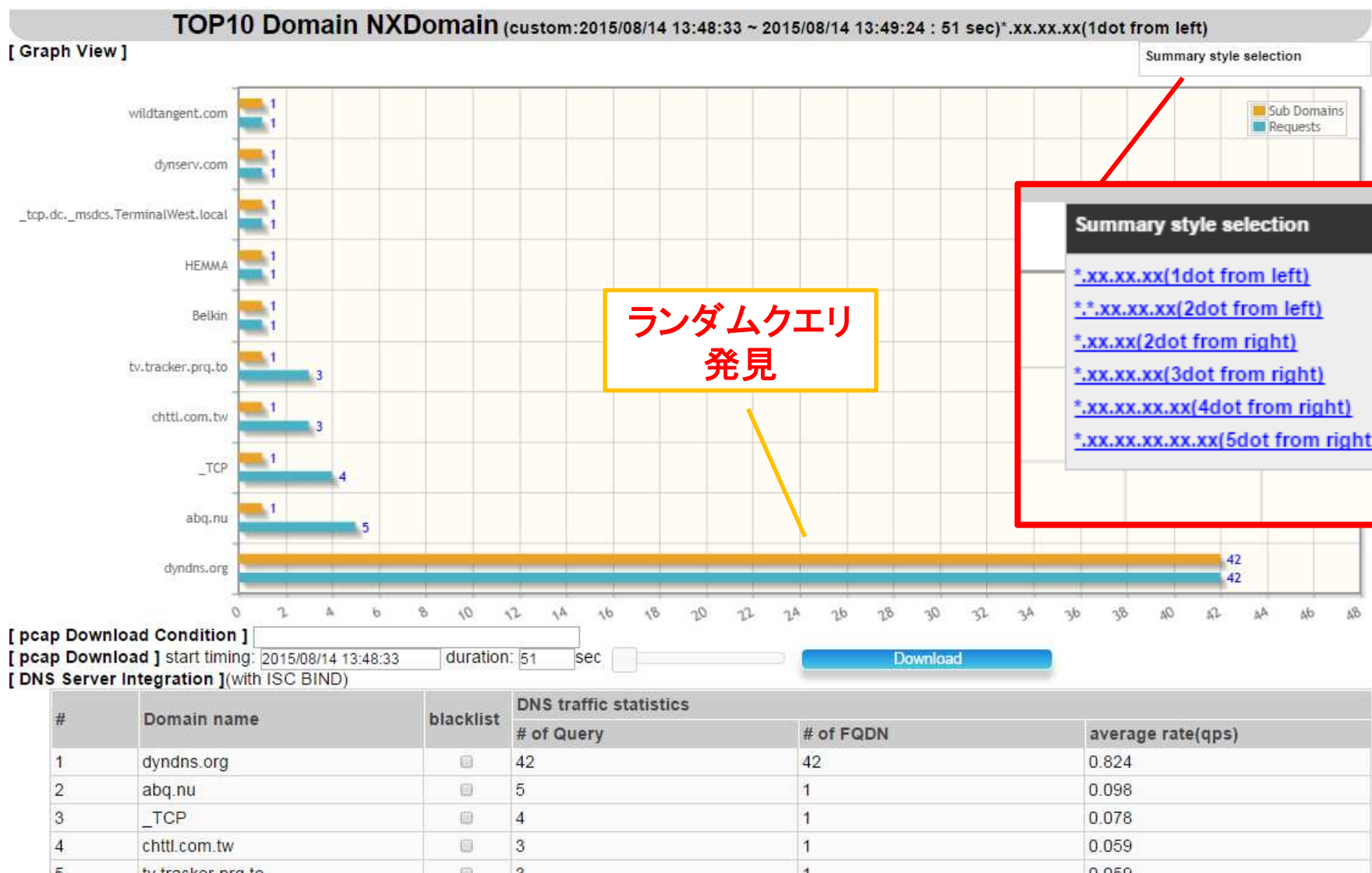
なんか1号機だけ処理多くない？

DNSサーバの仕事量の配合が見えました(偏りも見える)



7. 最近の活用例

水責めの存在も、これなら、けっこうさっくり見えました



7. 最近の活用例

水責めの存在も、これなら、けっこうさっくり見えました



pcap check

[pcap Information]

start time : 2015/08/21 09:58:11
duration : 68 sec
condition : [dyndns.org]

All traffic

pcap size : [822,777] packets
pcap size : [151,697,691] bytes
condition : []

Please check pcap file size.

[pcap Download]

Download

All NXDomain packets

pcap size : [62,344] packets
pcap size : [11,094,801] bytes
condition : [-n 17=3]

Please check pcap file size.

[pcap Download]

Download

Specific condition

pcap size : [43] packets
pcap size : [6,321] bytes
condition : [-n '17=3 7=*dyndns.org']

Please check pcap file size.

[pcap Download]

Download

ランダムクエリの
内容をpcapで確認

いろんな切り口で
pcapが切り出せます

back

1 : protocol number
2 : src IP
3 : dst IP
7 : FQDN
13 : DNS ID
14 : DNS Query / Response
(14=0 : Query)
(14=1 : Response)
15 : DNS Recursion Desired
(15=0 : not Desired)
(15=1 : Desired)
16 : DNS Recursion Available
(16=0 : not Available)
(16=1 : Available)
17 : DNS RCODE
(17=0 : NoError)
(17=2 : ServFail)
(17=3 : NXDomain)
(17=5 : Refused)
19 : DNS Resource Record Ty
(19=1 : A record)
(19=2 : NS record)...

8. まとめ(DNSサーバ運用の場面で変化したこと)

1. 速やかに、インシデントに気づく
⇒ 通知機構を作れてないけど、
見ればわかるようになった
2. 速やかに、起こっている内容について理解する
⇒ 切り口を変えつつ分析できるので、
状況が把握しやすくなった
3. 速やかに、対策を実施する
⇒ 絞り込んだpcapが取れるので、裏を取るときとかの
つらさが減った

Trafficの可視化(DNSの可視化)

ユーザ登録 : 必要
利用 : 無償でOK

作ったもの: DNS viewer

公開場所 : http://tapas.terilogy.com/projects/dns_viewer

momentum
DNS viewer
~ Packet Capture for Everywhere ~

probe
1Uprobe
172.16.183.74

Trend

- Interface Traffic
- Response Time
- Request / Response
- Request / Response(Recursion)
- Request / Response(Cache)
- RR TYPE
- Response - RCODE
- Response - ServFail
- Response - NXDomain

management

Logout

