Now the CNAME and A records are stored as separate events, and we won't know the cname of which domain. It would be great if this could be tracked. Guess this holds true for MX records as well.

For an example see below. I looked up www.geocities.com, which is a cname for geocities.com. The DNS server supplied additional RRs in the response which included the A record. All of them can be tied together by the same DNS transaction ID and also the chain of rrname -> rdata -> rrname -> rdata.

For example in the EVE log below we see:

- rrname: www.geocities.com, rdata: geocities.com (rtype CNAME)
- rrname: geocities.com, rdata: 98.137.201.117 (rtype A)

Can you take a look at the changes in version 2.1beta4 and see if they address your feature?

#2 - 07/07/2015 01:59 AM - Victor Julien
- Status changed from New to Closed

#3 - 08/12/2015 02:23 PM - Lucky b56
I someone missed the updates. Thanks, this works.

#4 - 08/12/2015 02:24 PM - Lucky b56
I somehow missed the updates. Thanks, this works.