Probing Open Recursive Name Servers

John Kristoff

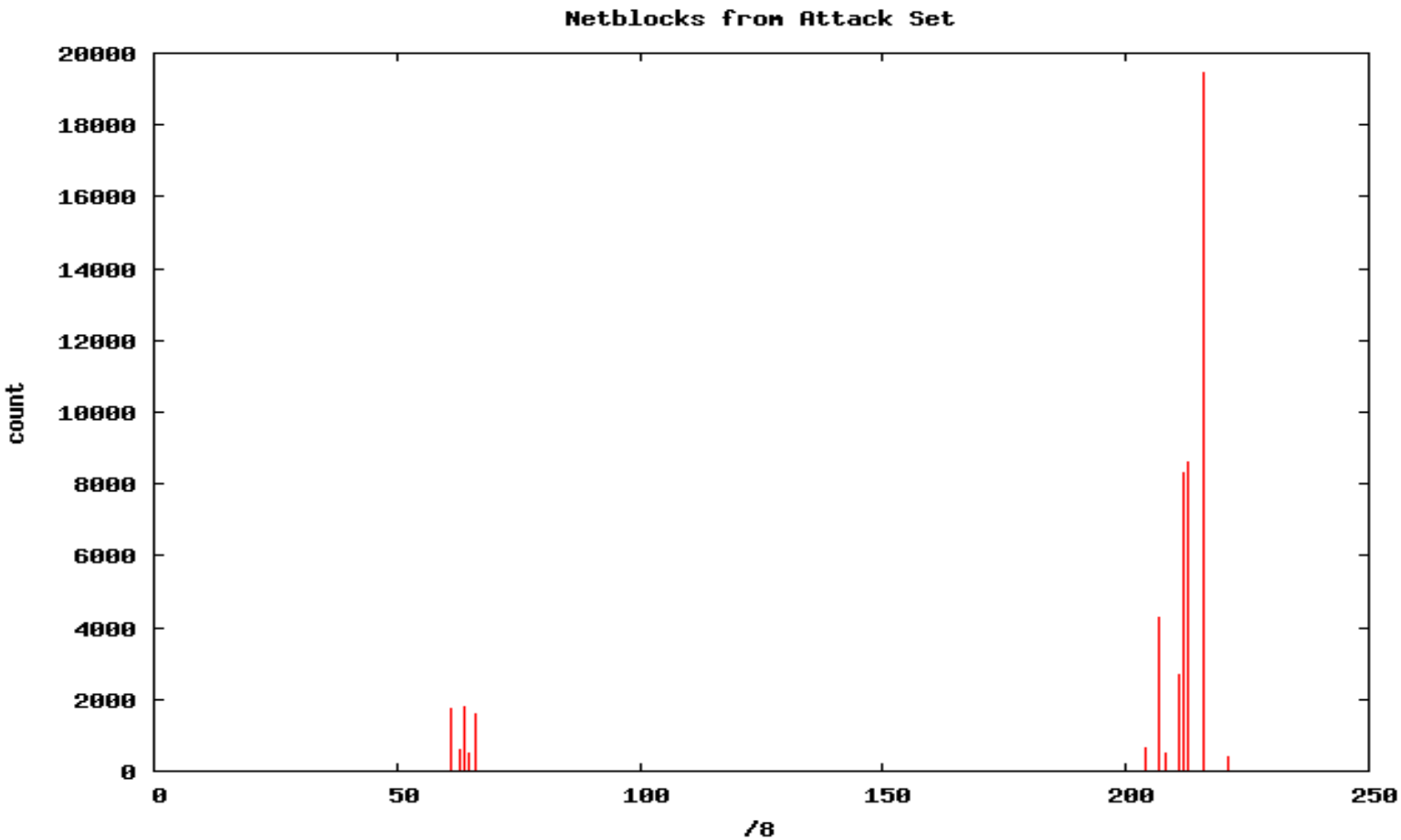
jtk@ultradns.net

NANOG 37 NSP-Security BoF

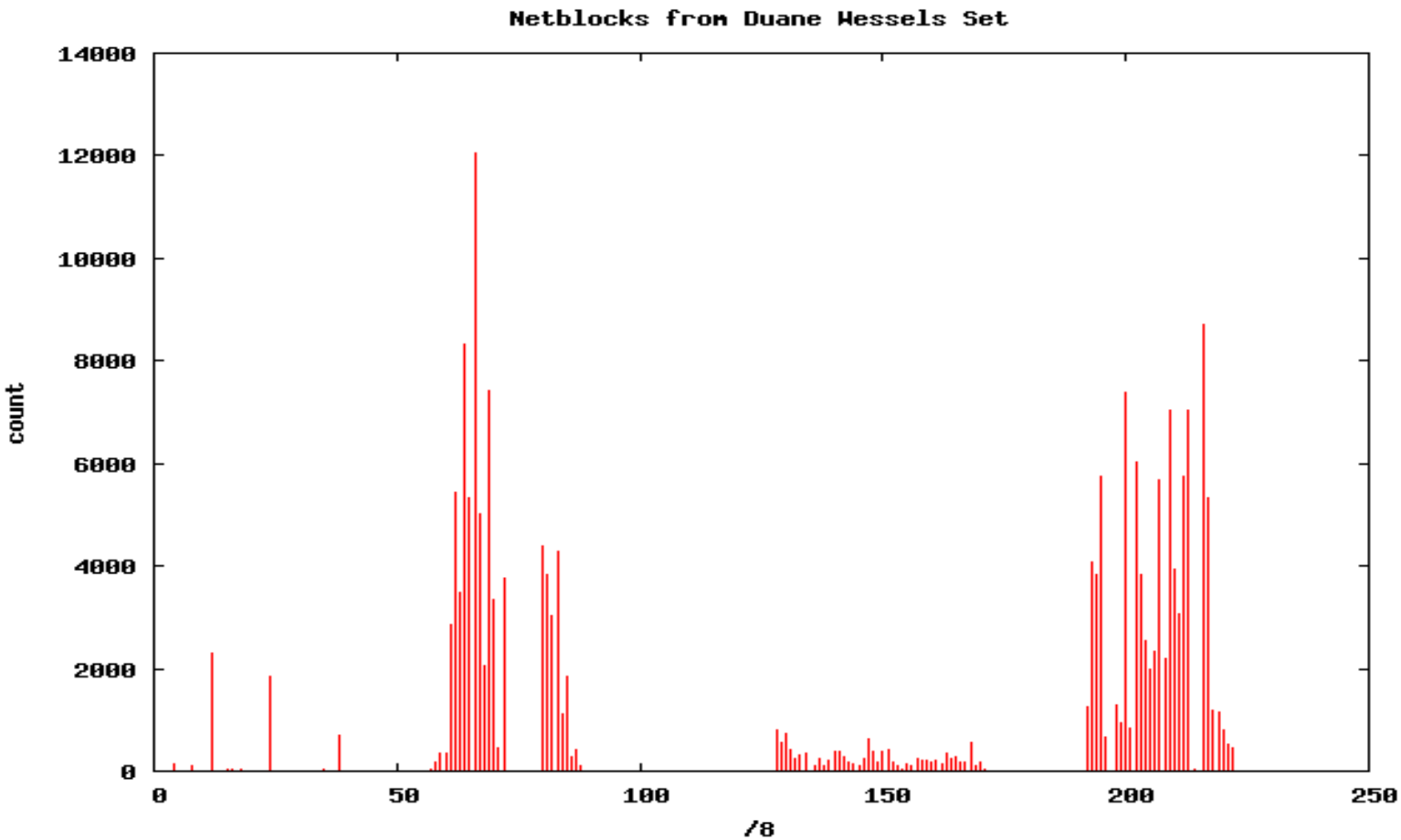
ORNS Candidate Data Sets

- 51,196 reflector attack, Feb. 2006
- 191,966 ORNS from Duane Wessels, March 2006
- 2,660,229 somethings querying us, March 2006

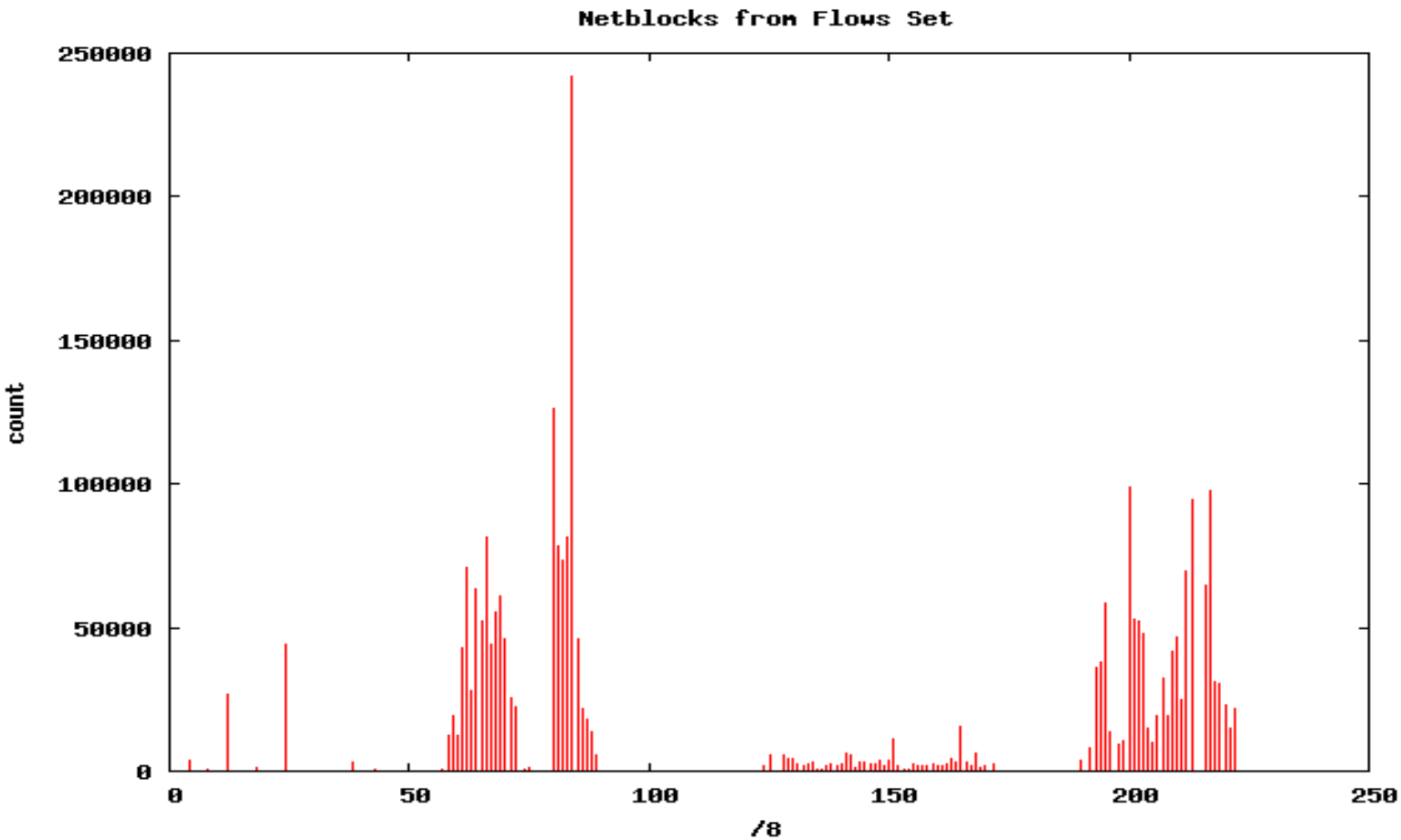
Netblocks - Attack Set



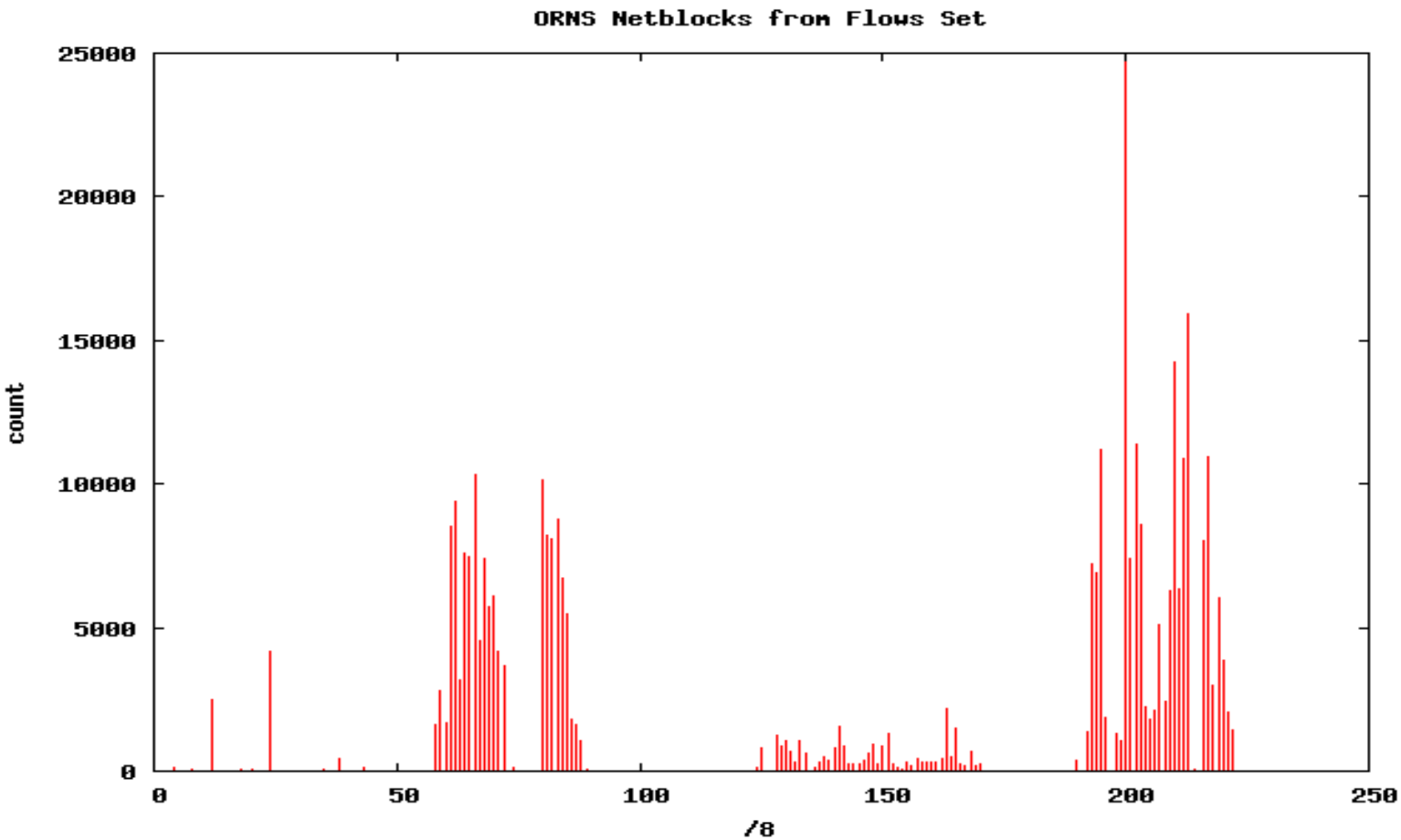
Netblocks - Duane's Set



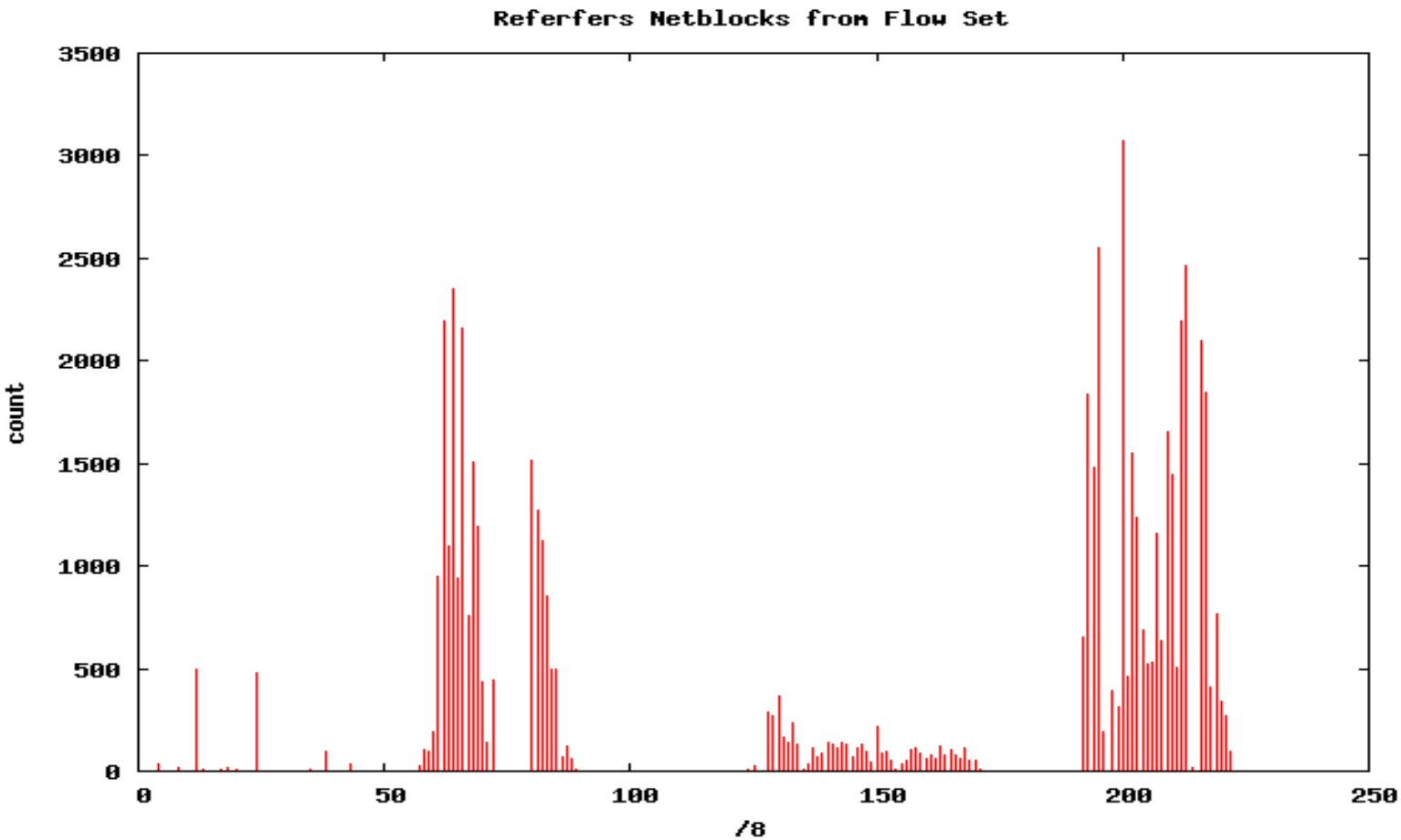
Netblocks - Our Flows



ORNS Netblocks - Our Flows (~14%)



Referrer Netblocks - Our flows (~2%)



Filtering in the Presence of Hidden ORNSs

- How many ORNSs are out there lurking?
- The CPE ORNSs do not reveal themself until an attack
- Only two of the attack addresses seen in flows set
- Generic port 53 filtering/limiting and whitelisting?
- Do we do a continual all netblocks ORNS scan?

Multifaceted ORNS Probing

- Query for whoareyou.ultradns.net
- Query for whoami.ultradns.net
- Query again for whoami.ultradns.net
- Query for unique, but bogus TLD
- Fingerprint with fpdns
- Query for unique name for a zone I control *

Remote Probing Challenges

- Recursion available (ra) bit is an unreliable indicator
- Non-existent TLD query doesn't always result in NXDOMAIN
- Low or zero TTL adherence is not guaranteed
- High-speed querying and timeouts
- Unexpected answer due to configuration or implementation

Caching Weirdness

```
$ dig @61.46.219.237 whoareyou.ultradns.net +noall +answer

; <<>> DiG 9.2.2 <<>> @61.46.219.237 whoareyou.ultradns.net +noall +answer
;; global options:  printcmd
whoareyou.ultradns.net. 0       IN      A       204.74.96.5

$ dig @61.46.219.237 whoareyou.ultradns.net +noall +answer

; <<>> DiG 9.2.2 <<>> @61.46.219.237 whoareyou.ultradns.net +noall +answer
;; global options:  printcmd
whoareyou.ultradns.net. 4294967292 IN   A       204.74.96.5
```

Alternate Root

```
$ dig @211.220.209.3 bogus-tld +noall +answer +authority

; <<>> DiG 9.2.2 <<>> @211.220.209.3 bogus-tld +noall +answer +authority
;; global options:  printcmd
realname.               86400   IN      A       211.106.67.200
realname.               86400   IN      NS      update-psi.netpia.com.
```

Wildcard

```
$ dig @213.30.189.132 nanug.org +noall +answer

; <<>> DiG 9.2.2 <<>> @213.30.189.132 nanug.org +noall +answer
;; global options:  printcmd
nanug.org.              10000   IN      A       62.210.183.75
nanug.org.              10000   IN      TXT     "toto"
```

Flags and Inconsistency

```
$ dig @213.215.76.84 +noall +comments +answer www.nanog.org
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52909
;; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

$ dig @213.215.76.84 +noall +comments +answer www.nanog.org
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43523
;; flags: qr; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; ANSWER SECTION:
www.nanog.org.          86392   IN      A       198.108.1.5
```

Query Amplification and Aggression?

```
Auth Server #1
client 209.63.146.65#37695: query: researchprobe-3632192887.example.org IN A -E
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -E
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
Auth Server #2
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -E
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -E
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
```

Bad Defaults

```
$ dig @202.146.225.194 bogus-tld +noall +comments +answer

; <<>> DiG 9.2.2 <<>> @202.146.225.194 bogus-tld +noall +comments +answer
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30140
;; flags: qr; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; ANSWER SECTION:
bogus-tld.              3600    IN      A       10.61.32.1
```

References

- http://public.oarci.net/files/wessels-openresolvers.pdf
- http://dns.measurement-factory.com/cgi-bin/openresolvercheck.pl
- http://cc.uoregon.edu/cnews/winter2006/recursive.htm
- http://www.icann.org/committees/security/dns-ddos-advisory-31mar06.pdf
- http://layer9.com/ jtk/tmp/dns-fp.txt
- http://layer9.com/ jtk/tmp/dns-id.txt