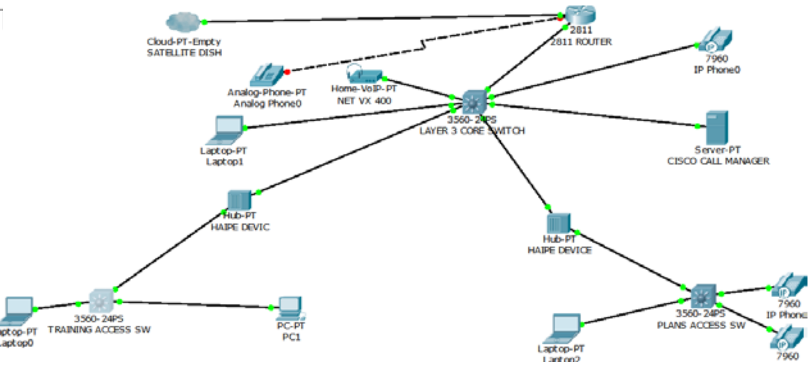
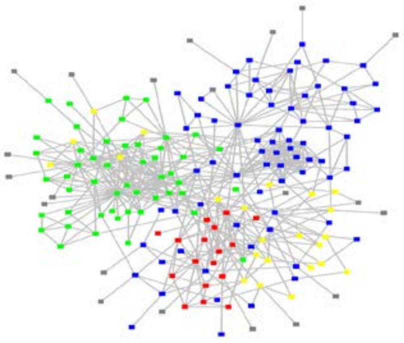
Exceptional service in the national interest

Sandia National Laboratories





Network Anomaly Detection

Dylan Hutchison

Advisor: Levi Lloyd

Summer 2013

SAND #2013-5904C

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Data Sources

Application Level

Low Level

Email Attachments

HTTP Traffic

Known Spam Lists

DNS Lookups

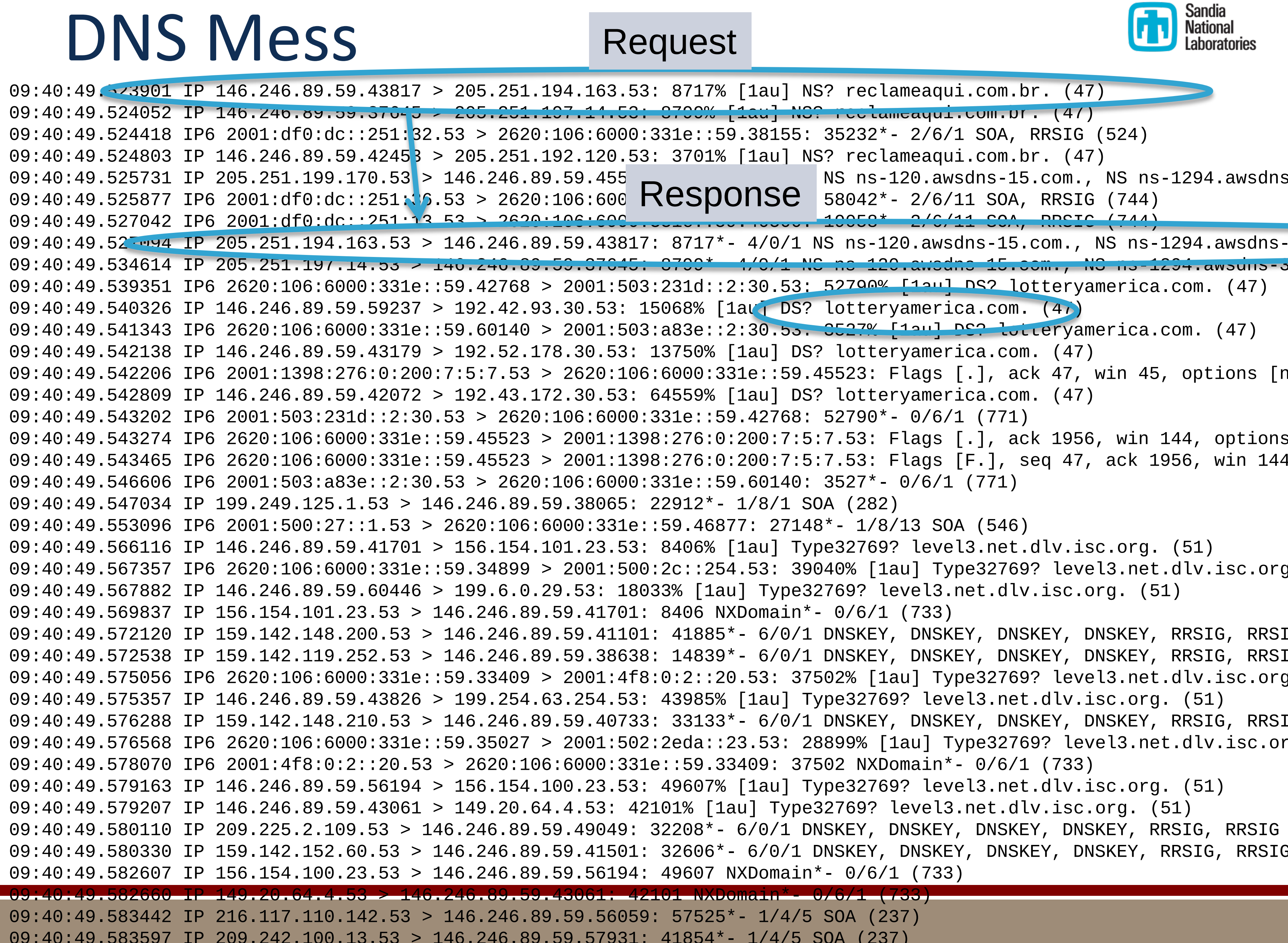
Netflow Data

ARP Requests

DNS Mess

```
09:40:49.523901 IP 146.246.89.59.43817 > 205.251.194.163.53: 8717% [1au] NS? reclameaqui.com.br. (47)
09:40:49.524052 IP 146.246.89.59.37645 > 205.251.197.14.53: 8799% [1au] NS? reclameaqui.com.br. (47)
09:40:49.524418 IP6 2001:df0:dc::251:32.53 > 2620:106:6000:331e::59.38155: 35232*- 2/6/1 SOA, RRSIG (524)
09:40:49.524803 IP 146.246.89.59.42453 > 205.251.192.120.53: 3701% [1au] NS? reclameaqui.com.br. (47)
09:40:49.525731 IP 205.251.199.170.53 > 146.246.89.59.45523: 40535*- 4/0/1 NS ns-120.awsdns-15.com., NS ns-1294.awsdns
09:40:49.525877 IP6 2001:df0:dc::251:36.53 > 2620:106:6000:331e::59.59596: 58042*- 2/6/11 SOA, RRSIG (744)
09:40:49.527042 IP6 2001:df0:dc::251:13.53 > 2620:106:6000:331e::59.40500: 19058*- 2/6/11 SOA, RRSIG (744)
09:40:49.527094 IP 205.251.194.163.53 > 146.246.89.59.43817: 8717*- 4/0/1 NS ns-120.awsdns-15.com., NS ns-1294.awsdns-
09:40:49.534614 IP 205.251.197.14.53 > 146.246.89.59.37645: 8799*- 4/0/1 NS ns-120.awsdns-15.com., NS ns-1294.awsdns-3
09:40:49.539351 IP6 2620:106:6000:331e::59.42768 > 2001:503:231d::2:30.53: 52790% [1au] DS? lotteryamerica.com. (47)
09:40:49.540326 IP 146.246.89.59.59237 > 192.42.93.30.53: 15068% [1au] DS? lotteryamerica.com. (47)
09:40:49.541343 IP6 2620:106:6000:331e::59.60140 > 2001:503:a83e::2:30.53: 3527% [1au] DS? lotteryamerica.com. (47)
09:40:49.542138 IP 146.246.89.59.43179 > 192.52.178.30.53: 13750% [1au] DS? lotteryamerica.com. (47)
09:40:49.542206 IP6 2001:1398:276:0:200:7:5:7.53 > 2620:106:6000:331e::59.45523: Flags [.], ack 47, win 45, options [n
09:40:49.542809 IP 146.246.89.59.42072 > 192.43.172.30.53: 64559% [1au] DS? lotteryamerica.com. (47)
09:40:49.543202 IP6 2001:503:231d::2:30.53 > 2620:106:6000:331e::59.42768: 52790*- 0/6/1 (771)
09:40:49.543274 IP6 2620:106:6000:331e::59.45523 > 2001:1398:276:0:200:7:5:7.53: Flags [.], ack 1956, win 144, options
09:40:49.543465 IP6 2620:106:6000:331e::59.45523 > 2001:1398:276:0:200:7:5:7.53: Flags [F.], seq 47, ack 1956, win 144
09:40:49.546606 IP6 2001:503:a83e::2:30.53 > 2620:106:6000:331e::59.60140: 3527*- 0/6/1 (771)
09:40:49.547034 IP 199.249.125.1.53 > 146.246.89.59.38065: 22912*- 1/8/1 SOA (282)
09:40:49.553096 IP6 2001:500:27::1.53 > 2620:106:6000:331e::59.46877: 27148*- 1/8/13 SOA (546)
09:40:49.566116 IP 146.246.89.59.41701 > 156.154.101.23.53: 8406% [1au] Type32769? level3.net.dlv.isc.org. (51)
09:40:49.567357 IP6 2620:106:6000:331e::59.34899 > 2001:500:2c::254.53: 39040% [1au] Type32769? level3.net.dlv.isc.org
09:40:49.567882 IP 146.246.89.59.60446 > 199.6.0.29.53: 18033% [1au] Type32769? level3.net.dlv.isc.org. (51)
09:40:49.569837 IP 156.154.101.23.53 > 146.246.89.59.41701: 8406 NXDomain*- 0/6/1 (733)
09:40:49.572120 IP 159.142.148.200.53 > 146.246.89.59.41101: 41885*- 6/0/1 DNSKEY, DNSKEY, DNSKEY, RRSIG, RRSI
09:40:49.572538 IP 159.142.119.252.53 > 146.246.89.59.38638: 14839*- 6/0/1 DNSKEY, DNSKEY, DNSKEY, RRSIG, RRSI
09:40:49.575056 IP6 2620:106:6000:331e::59.33409 > 2001:4f8:0:2::20.53: 37502% [1au] Type32769? level3.net.dlv.isc.org
09:40:49.575357 IP 146.246.89.59.43826 > 199.254.63.254.53: 43985% [1au] Type32769? level3.net.dlv.isc.org. (51)
09:40:49.576288 IP 159.142.148.210.53 > 146.246.89.59.40733: 33133*- 6/0/1 DNSKEY, DNSKEY, DNSKEY, RRSIG, RRSI
09:40:49.576568 IP6 2620:106:6000:331e::59.35027 > 2001:502:2eda::23.53: 28899% [1au] Type32769? level3.net.dlv.isc.or
09:40:49.578070 IP6 2001:4f8:0:2::20.53 > 2620:106:6000:331e::59.33409: 37502 NXDomain*- 0/6/1 (733)
09:40:49.579163 IP 146.246.89.59.56194 > 156.154.100.23.53: 49607% [1au] Type32769? level3.net.dlv.isc.org. (51)
09:40:49.579207 IP 146.246.89.59.43061 > 149.20.64.4.53: 42101% [1au] Type32769? level3.net.dlv.isc.org. (51)
09:40:49.580110 IP 209.225.2.109.53 > 146.246.89.59.49049: 32208*- 6/0/1 DNSKEY, DNSKEY, DNSKEY, DNSKEY, RRSIG, RRSIG
09:40:49.580330 IP 159.142.152.60.53 > 146.246.89.59.41501: 32606*- 6/0/1 DNSKEY, DNSKEY, DNSKEY, DNSKEY, RRSIG, RRSIG
09:40:49.582607 IP 156.154.100.23.53 > 146.246.89.59.56194: 49607 NXDomain*- 0/6/1 (733)
09:40:49.582660 IP 149.20.64.4.53 > 146.246.89.59.43061: 42101 NXDomain*- 0/6/1 (733)
09:40:49.583442 IP 216.117.110.142.53 > 146.246.89.59.56059: 57525*- 1/4/5 SOA (237)
09:40:49.583597 IP 209.242.100.13.53 > 146.246.89.59.57931: 41854*- 1/4/5 SOA (237)
```

DNS Mess

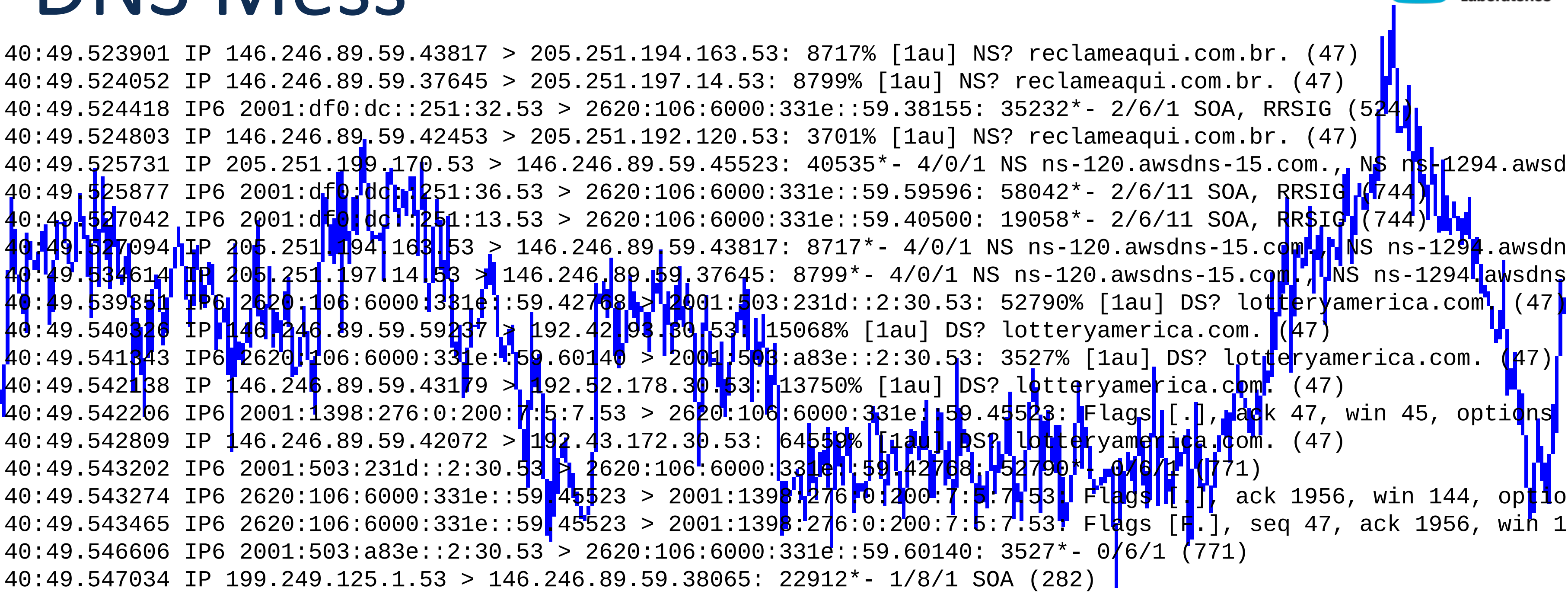


Request

Response

```
09:40:49.523901 IP 146.246.89.59.43817 > 205.251.194.163.53: 8717% [1au] NS? reclameaqui.com.br. (47)
09:40:49.524052 IP 146.246.89.59.37645 > 205.251.197.14.53: 8799% [1au] NS? reclameaqui.com.br. (47)
09:40:49.524418 IP6 2001:df0:dc::251:32.53 > 2620:106:6000:331e::59.38155: 35232*- 2/6/1 SOA, RRSIG (524)
09:40:49.524803 IP 146.246.89.59.42453 > 205.251.192.120.53: 3701% [1au] NS? reclameaqui.com.br. (47)
09:40:49.525731 IP 205.251.199.170.53 > 146.246.89.59.455[illegible] NS ns-120.awsdns-15.com., NS ns-1294.awsdns
09:40:49.525877 IP6 2001:df0:dc::251:36.53 > 2620:106:600[illegible] 58042*- 2/6/11 SOA, RRSIG (744)
09:40:49.527042 IP6 2001:df0:dc::251:13.53 > 2620:106:6000:331e::59.[illegible] 10058*- 2/6/11 SOA, RRSIG (744)
09:40:49.527094 IP 205.251.194.163.53 > 146.246.89.59.43817: 8717*- 4/0/1 NS ns-120.awsdns-15.com., NS ns-1294.awsdns-
09:40:49.534614 IP 205.251.197.14.53 > 146.246.89.59.37645: 8799*- 4/0/1 NS ns-120.awsdns-15.com., NS ns-1294.awsdns-3
09:40:49.539351 IP6 2620:106:6000:331e::59.42768 > 2001:503:231d::2:30.53: 52790% [1au] DS? lotteryamerica.com. (47)
09:40:49.540326 IP 146.246.89.59.59237 > 192.42.93.30.53: 15068% [1au] DS? lotteryamerica.com. (47)
09:40:49.541343 IP6 2620:106:6000:331e::59.60140 > 2001:503:a83e::2:30.53: 3527% [1au] DS? lotteryamerica.com. (47)
09:40:49.542138 IP 146.246.89.59.43179 > 192.52.178.30.53: 13750% [1au] DS? lotteryamerica.com. (47)
09:40:49.542206 IP6 2001:1398:276:0:200:7:5:7.53 > 2620:106:6000:331e::59.45523: Flags [.], ack 47, win 45, options [n
09:40:49.542809 IP 146.246.89.59.42072 > 192.43.172.30.53: 64559% [1au] DS? lotteryamerica.com. (47)
09:40:49.543202 IP6 2001:503:231d::2:30.53 > 2620:106:6000:331e::59.42768: 52790*- 0/6/1 (771)
09:40:49.543274 IP6 2620:106:6000:331e::59.45523 > 2001:1398:276:0:200:7:5:7.53: Flags [.], ack 1956, win 144, options
09:40:49.543465 IP6 2620:106:6000:331e::59.45523 > 2001:1398:276:0:200:7:5:7.53: Flags [F.], seq 47, ack 1956, win 144
09:40:49.546606 IP6 2001:503:a83e::2:30.53 > 2620:106:6000:331e::59.60140: 3527*- 0/6/1 (771)
09:40:49.547034 IP 199.249.125.1.53 > 146.246.89.59.38065: 22912*- 1/8/1 SOA (282)
09:40:49.553096 IP6 2001:500:27::1.53 > 2620:106:6000:331e::59.46877: 27148*- 1/8/13 SOA (546)
09:40:49.566116 IP 146.246.89.59.41701 > 156.154.101.23.53: 8406% [1au] Type32769? level3.net.dlv.isc.org. (51)
09:40:49.567357 IP6 2620:106:6000:331e::59.34899 > 2001:500:2c::254.53: 39040% [1au] Type32769? level3.net.dlv.isc.org
09:40:49.567882 IP 146.246.89.59.60446 > 199.6.0.29.53: 18033% [1au] Type32769? level3.net.dlv.isc.org. (51)
09:40:49.569837 IP 156.154.101.23.53 > 146.246.89.59.41701: 8406 NXDomain*- 0/6/1 (733)
09:40:49.572120 IP 159.142.148.200.53 > 146.246.89.59.41101: 41885*- 6/0/1 DNSKEY, DNSKEY, DNSKEY, RRSIG, RRSI
09:40:49.572538 IP 159.142.119.252.53 > 146.246.89.59.38638: 14839*- 6/0/1 DNSKEY, DNSKEY, DNSKEY, RRSIG, RRSI
09:40:49.575056 IP6 2620:106:6000:331e::59.33409 > 2001:4f8:0:2::20.53: 37502% [1au] Type32769? level3.net.dlv.isc.org
09:40:49.575357 IP 146.246.89.59.43826 > 199.254.63.254.53: 43985% [1au] Type32769? level3.net.dlv.isc.org. (51)
09:40:49.576288 IP 159.142.148.210.53 > 146.246.89.59.40733: 33133*- 6/0/1 DNSKEY, DNSKEY, DNSKEY, RRSIG, RRSI
09:40:49.576568 IP6 2620:106:6000:331e::59.35027 > 2001:502:2eda::23.53: 28899% [1au] Type32769? level3.net.dlv.isc.or
09:40:49.578070 IP6 2001:4f8:0:2::20.53 > 2620:106:6000:331e::59.33409: 37502 NXDomain*- 0/6/1 (733)
09:40:49.579163 IP 146.246.89.59.56194 > 156.154.100.23.53: 49607% [1au] Type32769? level3.net.dlv.isc.org. (51)
09:40:49.579207 IP 146.246.89.59.43061 > 149.20.64.4.53: 42101% [1au] Type32769? level3.net.dlv.isc.org. (51)
09:40:49.580110 IP 209.225.2.109.53 > 146.246.89.59.49049: 32208*- 6/0/1 DNSKEY, DNSKEY, DNSKEY, DNSKEY, RRSIG, RRSIG
09:40:49.580330 IP 159.142.152.60.53 > 146.246.89.59.41501: 32606*- 6/0/1 DNSKEY, DNSKEY, DNSKEY, RRSIG, RRSIG
09:40:49.582607 IP 156.154.100.23.53 > 146.246.89.59.56194: 49607 NXDomain*- 0/6/1 (733)
09:40:49.582660 IP 149.20.64.4.53 > 146.246.89.59.43061: 42101 NXDomain*- 0/6/1 (733)
09:40:49.583442 IP 216.117.110.142.53 > 146.246.89.59.56059: 57525*- 1/4/5 SOA (237)
09:40:49.583597 IP 209.242.100.13.53 > 146.246.89.59.57931: 41854*- 1/4/5 SOA (237)
```

DNS Mess



```
09:40:49.523901 IP 146.246.89.59.43817 > 205.251.194.163.53: 8717% [1au] NS? reclameaqui.com.br. (47)
09:40:49.524052 IP 146.246.89.59.37645 > 205.251.197.14.53: 8799% [1au] NS? reclameaqui.com.br. (47)
09:40:49.524418 IP6 2001:df0:dc::251:32.53 > 2620:106:6000:331e::59.38155: 35232*- 2/6/1 SOA, RRSIG (524)
09:40:49.524803 IP 146.246.89.59.42453 > 205.251.192.120.53: 3701% [1au] NS? reclameaqui.com.br. (47)
09:40:49.525731 IP 205.251.199.170.53 > 146.246.89.59.45523: 40535*- 4/0/1 NS ns-120.awsdns-15.com., NS ns-1294.awsdns
09:40:49.525877 IP6 2001:df0:dc::251:36.53 > 2620:106:6000:331e::59.59596: 58042*- 2/6/11 SOA, RRSIG (744)
09:40:49.527042 IP6 2001:df0:dc::251:13.53 > 2620:106:6000:331e::59.40500: 19058*- 2/6/11 SOA, RRSIG (744)
09:40:49.527094 IP 205.251.194.163.53 > 146.246.89.59.43817: 8717*- 4/0/1 NS ns-120.awsdns-15.com., NS ns-1294.awsdns-
09:40:49.534614 IP 205.251.197.14.53 > 146.246.89.59.37645: 8799*- 4/0/1 NS ns-120.awsdns-15.com., NS ns-1294.awsdns-3
09:40:49.539351 IP6 2620:106:6000:331e::59.42768 > 2001:503:231d::2:30.53: 52790% [1au] DS? lotteryamerica.com. (47)
09:40:49.540326 IP 146.246.89.59.59237 > 192.42.93.30.53: 15068% [1au] DS? lotteryamerica.com. (47)
09:40:49.541343 IP6 2620:106:6000:331e::59.60140 > 2001:503:a83e::2:30.53: 3527% [1au] DS? lotteryamerica.com. (47)
09:40:49.542138 IP 146.246.89.59.43179 > 192.52.178.30.53: 13750% [1au] DS? lotteryamerica.com. (47)
09:40:49.542206 IP6 2001:1398:276:0:200:7:5:7.53 > 2620:106:6000:331e::59.45523: Flags [.], ack 47, win 45, options [n
09:40:49.542809 IP 146.246.89.59.42072 > 192.43.172.30.53: 64559% [1au] DS? lotteryamerica.com. (47)
09:40:49.543202 IP6 2001:503:231d::2:30.53 > 2620:106:6000:331e::59.42768: 52790*- 0/6/1 (771)
09:40:49.543274 IP6 2620:106:6000:331e::59.45523 > 2001:1398:276:0:200:7:5:7.53: Flags [.], ack 1956, win 144, options
09:40:49.543465 IP6 2620:106:6000:331e::59.45523 > 2001:1398:276:0:200:7:5:7.53: Flags [F.], seq 47, ack 1956, win 144
09:40:49.546606 IP6 2001:503:a83e::2:30.53 > 2620:106:6000:331e::59.60140: 3527*- 0/6/1 (771)
09:40:49.547034 IP 199.249.125.1.53 > 146.246.89.59.38065: 22912*- 1/8/1 SOA (282)
09:40:49.553096 IP6 200                                                         )
09:40:49.566116 IP 146.                                                         .dlv.isc.org. (51)
09:40:49.567357 IP6 262                                                         9? level3.net.dlv.isc.org
09:40:49.567882 IP 146.                                                         v.isc.org. (51)
09:40:49.569837 IP 156.
09:40:49.572120 IP 159.                                                         SKEY, DNSKEY, RRSIG, RRSI
09:40:49.572538 IP 159.                                                         SKEY, DNSKEY, RRSIG, RRSI
09:40:49.575056 IP6 262                                                         9? level3.net.dlv.isc.org
09:40:49.575357 IP 146.246.89.59.43826 > 199.254.63.254.53: 43985% [1au] Type32769? level3.net.dlv.isc.org. (51)
09:40:49.576288 IP 159.142.148.210.53 > 146.246.89.59.40733: 33133*- 6/0/1 DNSKEY, DNSKEY, DNSKEY, DNSKEY, RRSIG, RRSI
09:40:49.576568 IP6 2620:106                                                    ype32769? level3.net.dlv.isc.or
09:40:49.578070 IP6 2001:4f8                                                    0/6/1 (733)
09:40:49.579163 IP 146.246.8                                                    el3.net.dlv.isc.org. (51)
09:40:49.579207 IP 146.246.89.59.43061 > 149.20.64.4.53: 42101% [1au] Type32769? level3.net.dlv.isc.org. (51)
09:40:49.580110 IP 209.225.2.109.53 > 146.246.89.59.49049: 32208*- 6/0/1 DNSKEY, DNSKEY, DNSKEY, DNSKEY, RRSIG, RRSIG
09:40:49.580330 IP 159.142.152.60.53 > 146.246.89.59.41501: 32606*- 6/0/1 DNSKEY, DNSKEY, DNSKEY, DNSKEY, RRSIG, RRSIG
09:40:49.582607 IP 156.154.100.23.53 > 146.246.89.59.56194: 49607 NXDomain*- 0/6/1 (733)
09:40:49.582660 IP 149.20.64.4.53 > 146.246.89.59.43061: 42101 NXDomain*- 0/6/1 (733)
09:40:49.583442 IP 216.117.110.142.53 > 146.246.89.59.56059: 57525*- 1/4/5 SOA (237)
09:40:49.583597 IP 209.242.100.13.53 > 146.246.89.59.57931: 41854*- 1/4/5 SOA (237)
```

Goal: Find signal of malicious IPs/Domains

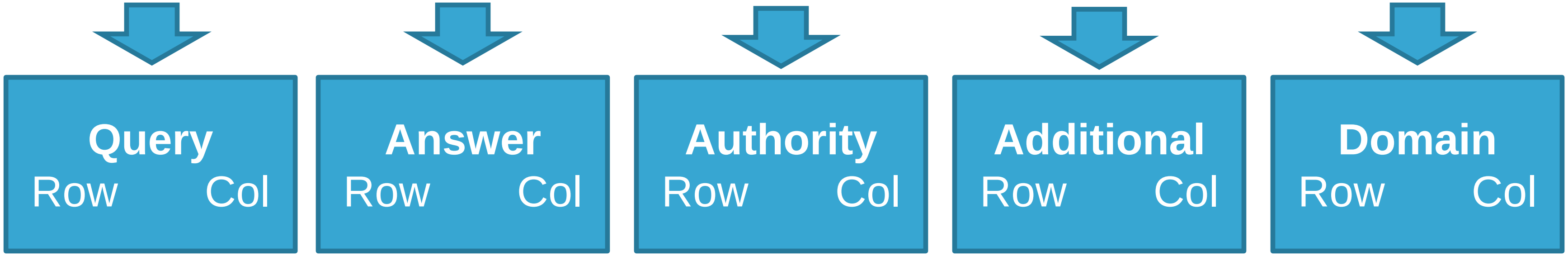
Strip Noise & Add Structure

DNS Data: Parsing

```
09:40:49.523901 IP 146.246.89.59.43817 > 205.251.194.163.53: 8717% [1au] NS? reclameaqui.com.br. (47)
09:40:49.524052 IP 146.246.89.59.37645 > 205.251.197.14.53: 8799% [1au] NS? reclameaqui.com.br. (47)
09:40:49.524418 IP6 2001:df0:dc::251:32.53 > 2620:106:6000:331e::59.38155: 35232*- 2/6/1 SOA, RRSIG (524)
09:40:49.524803 IP 146.246.89.59.42453 > 205.251.192.120.53: 3701% [1au] NS? reclameaqui.com.br. (47)
09:40:49.525731 IP 205.251.199.170.53 > 146.246.89.59.45523: 40535*- 4/0/1 NS ns-120.awsdns-15.com., NS
ns-1294.awsdns-33.org., NS ns-1962.awsdns-53.co.uk., NS ns-675.awsdns-20.net. (187)
09:40:49.525877 IP6 2001:df0:dc::251:36.53 > 2620:106:6000:331e::59.59596: 58042*- 2/6/11 SOA, RRSIG
(744)
09:40:49.527042 IP6 2001:df0:dc::251:13.53 > 2620:106:6000:331e::59.40500: 19058*- 2/6/11 SOA, RRSIG
(744)
09:40:49.527094 IP 205.251.194.163.53 > 146.246.89.59.43817: 8717*- 4/0/1 NS ns-120.awsdns-15.com., NS
ns-1294.awsdns-33.org., NS ns-1962.                                    0.net. (187)
09:40:49.534614 IP 205.251.197.14.5                                    1 NS ns-120.awsdns-15.com., NS ns-
1294.awsdns-33.org., NS ns-1962.aws                                    et. (187)
09:40:49.539351 IP6 2620:106:6000:3                                    53: 52790% [1au] DS?
lotteryamerica.com. (47)
09:40:49.540326 IP 146.246.89.59.59                                    DS? lotteryamerica.com. (47)
09:40:49.541343 IP6 2620:106:6000:3                                    53: 3527% [1au] DS?
lotteryamerica.com. (47)
09:40:49.542138 IP 146.246.89.59.43179 > 192.52.178.30.53: 13750% [1au] DS? lotteryamerica.com. (47)
09:40:49.542206 IP6 2001:1398:276:0:200:7:5:7.53 > 2620:106:6000:331e::59.45523: Flags [.], ack 47, win
45, options [nop,nop,TS val 2491795726 ecr 2700282080], length 0
09:40:49.542809 IP 146.246.89.59.42072 > 192.43.172.30.53: 64559% [1au] DS? lotteryamerica.com. (47)
09:40:49.543202 IP6 2001:503:231d::2:30.53 > 2620:106:6000:331e::59.42768: 52790*- 0/6/1 (771)
09:40:49.543274 IP6 2620:106:6000:331e::59.45523 > 2001:1398:276:0:200:7:5:7.53: Flags [.], ack 1956, win
144, options [nop,nop,TS val 2700282116 ecr 2491795726], length 0
09:40:49.543465 IP6 2620:106:6000:331e::59.45523 > 2001:1398:276:0:200:7:5:7.53: Flags [F.], seq 47, ack
1956, win 144, options [nop,nop,TS val 2700282116 ecr 2491795726], length 0
09:40:49.546606 IP6 2001:503:a83e::2:30.53 > 2620:106:6000:331e::59.60140: 3527*- 0/6/1 (771)
09:40:49.547034 IP 199.249.125.1.53 > 146.246.89.59.38065: 22912*- 1/8/1 SOA (282)
```

1. Strip noise

2. Structure



Query
Row Col

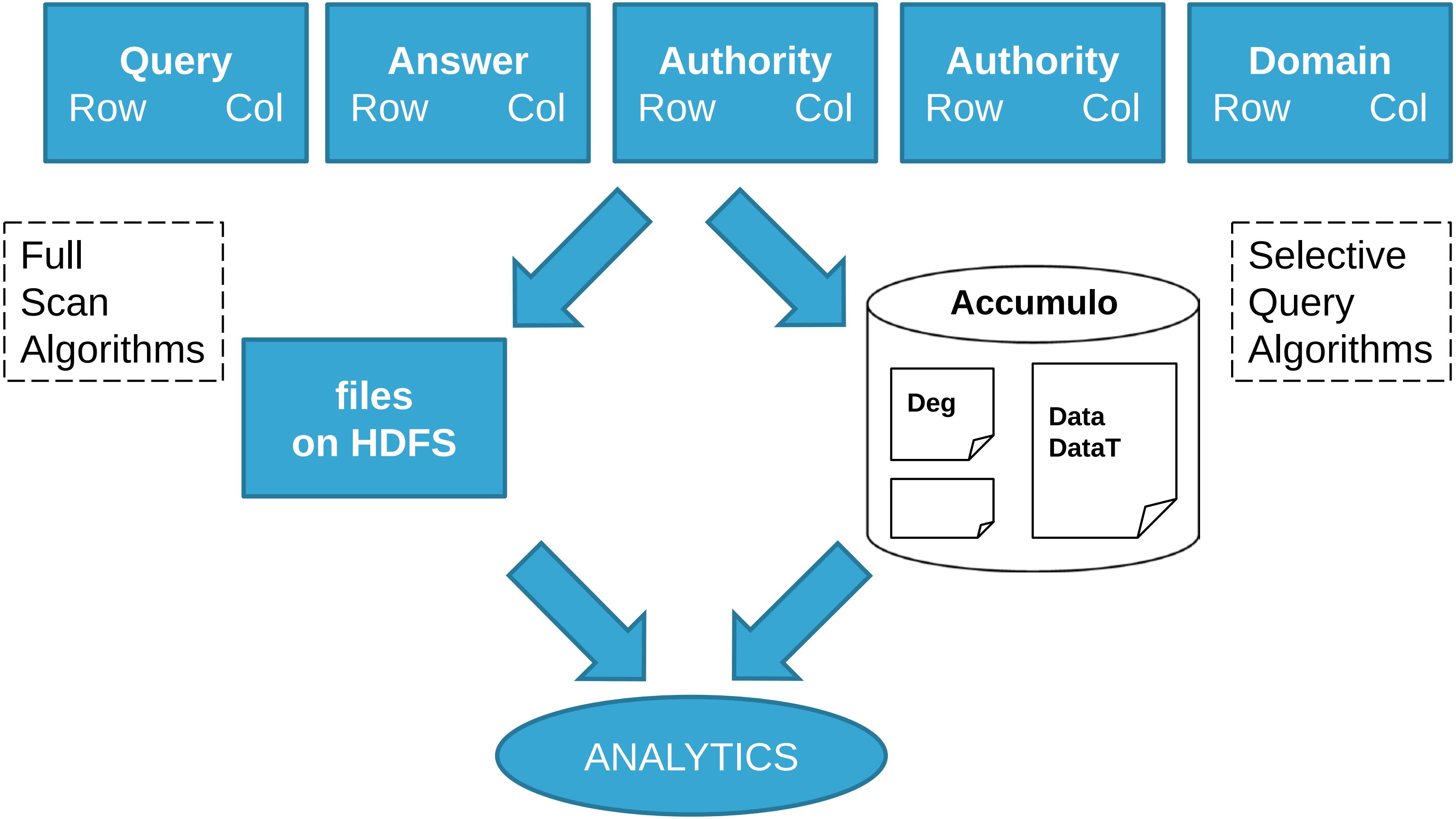
Answer
Row Col

Authority
Row Col

Additional
Row Col

Domain
Row Col

DNS Data: Table Ingest



Accumulo Schema

Exploded Schema	src_ip|10.0.2.8	src_ip|192.168.1.36	Qhost|.com.google	Qhost|.ly.bit	Qhost|.com.yahoo
lookup_hash|001	1	1	0	0	1
lookup_hash|002	0	1	1	0	0
lookup_hash|003	1	0	0	1	0

- Indexing Across all Variables
- Server-Side Computation
  - Automatic Degree Counts (separate table)

➔ Flexible Analytics

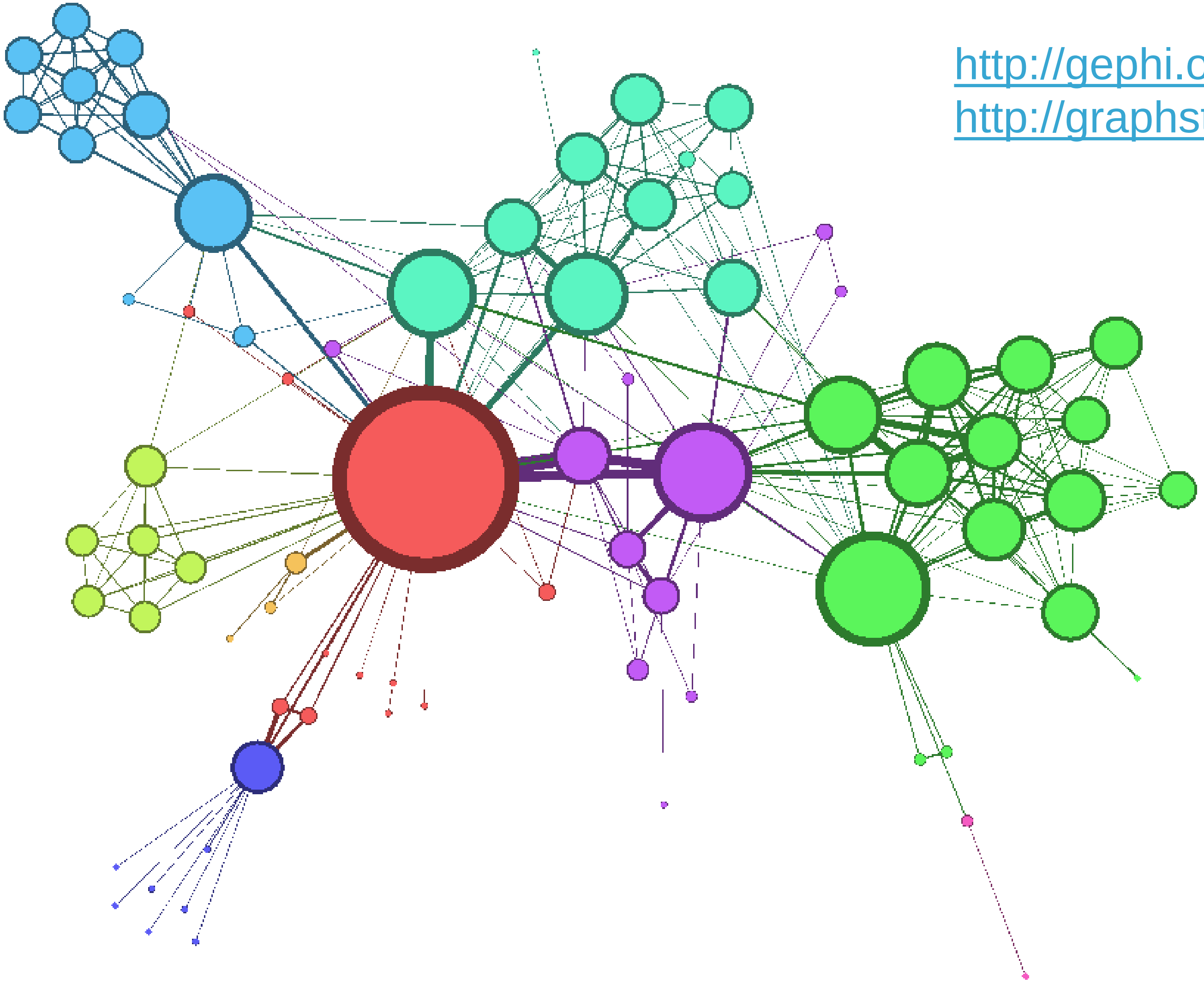
Queries

- What are the 4 most frequently returned answers? What were the original requests?
- Find all lookups with TTLs < 10
- Find 10 domains with most unique associated IPs
  - For IPv4, IPv6, both
- Find top 10 queried domains on May 1, 9:10 – 9:19am

Future Work

- Flexibility first, to identify features
  1. Expert Analysis
  2. Machine Learning
- Efficiency next, specializing on key features
- Run on real data!

New angle: Visualization



http://gephi.org/
http://graphstream-project.org/