Troubleshooting DNS

Troubleshooting DNS

- Understanding the Domain Name System (DNS)
- Wireshark and DNS
  - Used to capture the conversation
  - Can see the queries, recursion, and other events
  - Will capture UDP and TCP port 53
- Ports
  - UDP 53 (standard query)
  - TCP 53 zone transfer

Troubleshooting DNS

Filter: dns Expression... Clear Apply Save

No.	Time	UTC	Source	Destination	Protocol	Info
8	0.000000000	2014-09-28 21:47:38.069976000	192.168.1.13	192.168.1.1	DNS	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
9	0.005342000	2014-09-28 21:47:38.075318000	192.168.1.1	192.168.1.13	DNS	Standard query response 0x0001 PTR Wireless_Broadband_Router.home
12	1.334987000	2014-09-28 21:47:39.410305000	192.168.1.13	192.168.1.1	DNS	Standard query 0x505f NS nslijhs.net
13	0.010665000	2014-09-28 21:47:39.420970000	192.168.1.1	192.168.1.13	DNS	Standard query response 0x505f NS nsex2.northshorelij.com NS nsex2.ns
14	0.003638000	2014-09-28 21:47:39.424608000	192.168.1.13	69.27.229.12	DNS	Standard query 0x25da SOA nslijhs.net
15	0.012963000	2014-09-28 21:47:39.437571000	69.27.229.12	192.168.1.13	DNS	Standard query response 0x25da SOA bcat02.nshs.edu
16	0.003984000	2014-09-28 21:47:39.441555000	192.168.1.13	10.170.171.1	DNS	Dynamic update 0x0288 SOA nslijhs.net
19	3.960918000	2014-09-28 21:47:43.402473000	192.168.1.13	192.168.1.1	DNS	Standard query 0x0002 A www.google.com.nslijhs.net
20	0.022950000	2014-09-28 21:47:43.425423000	192.168.1.1	192.168.1.13	DNS	Standard query response 0x0002 A 92.242.140.21
21	0.002752000	2014-09-28 21:47:43.428175000	192.168.1.13	192.168.1.1	DNS	Standard query 0x0003 AAAA www.google.com.nslijhs.net
22	0.015038000	2014-09-28 21:47:43.443213000	192.168.1.1	192.168.1.13	DNS	Standard query response 0x0003
23	1.003747000	2014-09-28 21:47:44.446960000	192.168.1.13	10.170.171.1	DNS	Dynamic update 0x0288 SOA nslijhs.net
25	6.093923000	2014-09-28 21:47:50.540883000	192.168.1.13	192.168.1.1	DNS	Standard query 0x0004 A www.ine.com.nslijhs.net
26	0.026380000	2014-09-28 21:47:50.567263000	192.168.1.1	192.168.1.13	DNS	Standard query response 0x0004 A 92.242.140.21
27	0.001789000	2014-09-28 21:47:50.569052000	192.168.1.13	192.168.1.1	DNS	Standard query 0x0005 AAAA www.ine.com.nslijhs.net
28	0.041698000	2014-09-28 21:47:50.610750000	192.168.1.1	192.168.1.13	DNS	Standard query response 0x0005
33	2.387026000	2014-09-28 21:47:52.997776000	192.168.1.13	192.168.1.1	DNS	Standard query 0xe0e0 A n2k3wb972prt01.nslijhs.net
34	0.021397000	2014-09-28 21:47:53.019173000	192.168.1.1	192.168.1.13	DNS	Standard query response 0xe0e0 A 92.242.140.21
35	0.003431000	2014-09-28 21:47:53.022604000	192.168.1.13	192.168.1.1	DNS	Standard query 0x5875 A n2k3wb972prt01.nslijhs.net
36	0.017015000	2014-09-28 21:47:53.039619000	192.168.1.1	192.168.1.13	DNS	Standard query response 0x5875 A 92.242.140.21
39	1.422199000	2014-09-28 21:47:54.461818000	192.168.1.13	10.170.171.1	DNS	Dynamic update 0x0288 SOA nslijhs.net
42	1.966222000	2014-09-28 21:47:56.428040000	192.168.1.13	192.168.1.1	DNS	Standard query 0x08fe A n2k3wb972prt01.nslijhs.net

Troubleshooting DNS

```
⊞ User Datagram Protocol, Src Port: 58157 (58157), Dst Port: 53 (53)
⊟ Domain Name System (query)
    [Response In: 20]
    Transaction ID: 0x0002
  ⊟ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊞ Queries
```

Questions?