Marcos Gomez

Sample from UDP

```
22:57:15.397158 IP (tos 0x0, ttl 64, id 3832, offset 0, flags [DF], proto UDP (17), length 72)
    192.168.254.15.32799 > dns1.cs.arizona.edu.domain: 42643+ PTR? 2.254.168.192.in-addr.arpa. (44)
22:57:15.400351 IP (tos 0x0, ttl 64, id 17290, offset 0, flags [none], proto UDP (17), length 149)
    dns1.cs.arizona.edu.domain > 192.168.254.15.32799: 42643 NXDomain 0/1/0 (121)
22:57:15.400678 IP (tos 0x0, ttl 64, id 3833, offset 0, flags [DF], proto UDP (17), length 73)
    192.168.254.15.59186 > dns1.cs.arizona.edu.domain: 60112+ PTR? 15.254.168.192.in-addr.arpa. (45)
22:57:15.401267 IP (tos 0x0, ttl 64, id 17291, offset 0, flags [none], proto UDP (17), length 150)
    dns1.cs.arizona.edu.domain > 192.168.254.15.59186: 60112 NXDomain 0/1/0 (122)
22:57:15.401596 IP (tos 0x10, ttl 64, id 23023, offset 0, flags [DF], proto TCP (6), length 444)
    192.168.254.15.ssh > 192.168.254.2.14794: Flags [P.], cksum 0x7f12 (incorrect -> 0xb882), seq 264:668, ack 1, win 49152, length 404
```

Sample from TCP

```
23:01:49.257971 IP (tos 0x10, ttl 64, id 23177, offset 0, flags [DF], proto TCP (6), length 444)
    192.168.254.15.ssh > 192.168.254.2.14794: Flags [P.], cksum 0x7f12 (incorrect -> 0x89fd), seq 264:668, ack 1, win 49152, length 404
23:01:49.258368 IP (tos 0x0, ttl 64, id 17575, offset 0, flags [none], proto TCP (6), length 40)
    192.168.254.2.14794 > 192.168.254.15.ssh: Flags [.], cksum 0x2f29 (correct), ack 668, win 65535, length 0
23:01:49.590088 IP (tos 0x10, ttl 64, id 20036, offset 0, flags [DF], proto TCP (6), length 92)
    192.168.254.15.ssh > 192.168.254.2.12263: Flags [P.], cksum 0x7db2 (incorrect -> 0x01df), seq 2809078072:2809078124, ack
4121095207, win 38912, length 52
23:01:49.590652 IP (tos 0x0, ttl 64, id 17576, offset 0, flags [none], proto TCP (6), length 40)
    192.168.254.2.12263 > 192.168.254.15.ssh: Flags [.], cksum 0x57cd (correct), ack 52, win 65535, length 0
23:01:50.259337 IP (tos 0x0, ttl 64, id 40152, offset 0, flags [DF], proto UDP (17), length 72)
    192.168.254.15.44751 > dns1.cs.arizona.edu.domain: 58004+ PTR? 231.69.12.192.in-addr.arpa. (44)
23:01:50.259597 IP (tos 0x10, ttl 64, id 23178, offset 0, flags [DF], proto TCP (6), length 172)
    192.168.254.15.ssh > 192.168.254.2.14794: Flags [P.], cksum 0x7e02 (incorrect -> 0xed4e), seq 668:800, ack 1, win 49152, length 132
```

When using UDP, there was a lot less traffic than TCP when looking at tcpdump. There also seemed to be more incorrect check sums when using TCP. When using UDP, it is more likely to see 'proto UDP(17)' in the tcpdump.