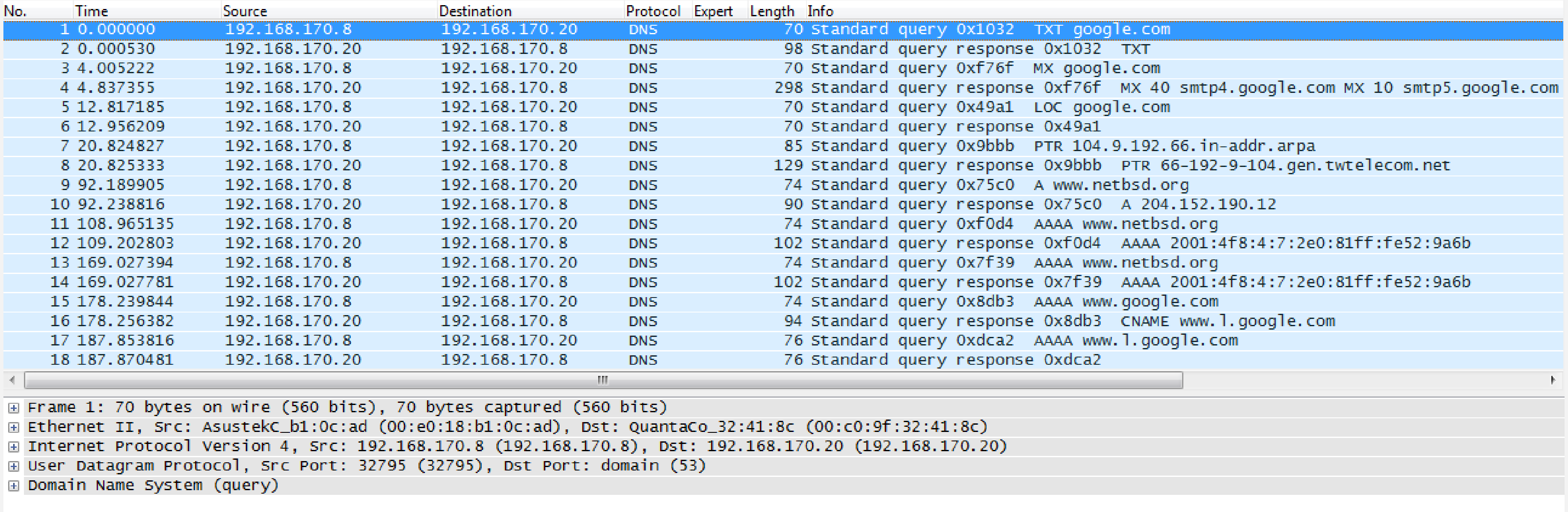
DNS Resolution Analysis

DNS Resolution Analysis

- **Resolution and DNS**
  - Clients make request by using a DNS name
  - If not configured locally (HOSTS), a DNS server is queried to provide needed information
  - When the client uses the FQDN, the resource can be found and accessed if available
- **What can be found with Wireshark?**
  - Failures in DNS from the client to the DNS server and beyond

DNS Resolution Analysis



No.	Time	Source	Destination	Protocol	Expert	Length	Info
1	0.000000	192.168.170.8	192.168.170.20	DNS		70	Standard query 0x1032 TXT google.com
2	0.000530	192.168.170.20	192.168.170.8	DNS		98	Standard query response 0x1032 TXT
3	4.005222	192.168.170.8	192.168.170.20	DNS		70	Standard query 0xf76f MX google.com
4	4.837355	192.168.170.20	192.168.170.8	DNS		298	Standard query response 0xf76f MX 40 smtp4.google.com MX 10 smtp5.google.com
5	12.817185	192.168.170.8	192.168.170.20	DNS		70	Standard query 0x49a1 LOC google.com
6	12.956209	192.168.170.20	192.168.170.8	DNS		70	Standard query response 0x49a1
7	20.824827	192.168.170.8	192.168.170.20	DNS		85	Standard query 0x9bbb PTR 104.9.192.66.in-addr.arpa
8	20.825333	192.168.170.20	192.168.170.8	DNS		129	Standard query response 0x9bbb PTR 66-192-9-104.gen.twtelecom.net
9	92.189905	192.168.170.8	192.168.170.20	DNS		74	Standard query 0x75c0 A www.netbsd.org
10	92.238816	192.168.170.20	192.168.170.8	DNS		90	Standard query response 0x75c0 A 204.152.190.12
11	108.965135	192.168.170.8	192.168.170.20	DNS		74	Standard query 0xf0d4 AAAA www.netbsd.org
12	109.202803	192.168.170.20	192.168.170.8	DNS		102	Standard query response 0xf0d4 AAAA 2001:4f8:4:7:2e0:81ff:fe52:9a6b
13	169.027394	192.168.170.8	192.168.170.20	DNS		74	Standard query 0x7f39 AAAA www.netbsd.org
14	169.027781	192.168.170.20	192.168.170.8	DNS		102	Standard query response 0x7f39 AAAA 2001:4f8:4:7:2e0:81ff:fe52:9a6b
15	178.239844	192.168.170.8	192.168.170.20	DNS		74	Standard query 0x8db3 AAAA www.google.com
16	178.256382	192.168.170.20	192.168.170.8	DNS		94	Standard query response 0x8db3 CNAME www.l.google.com
17	187.853816	192.168.170.8	192.168.170.20	DNS		76	Standard query 0xdca2 AAAA www.l.google.com
18	187.870481	192.168.170.20	192.168.170.8	DNS		76	Standard query response 0xdca2

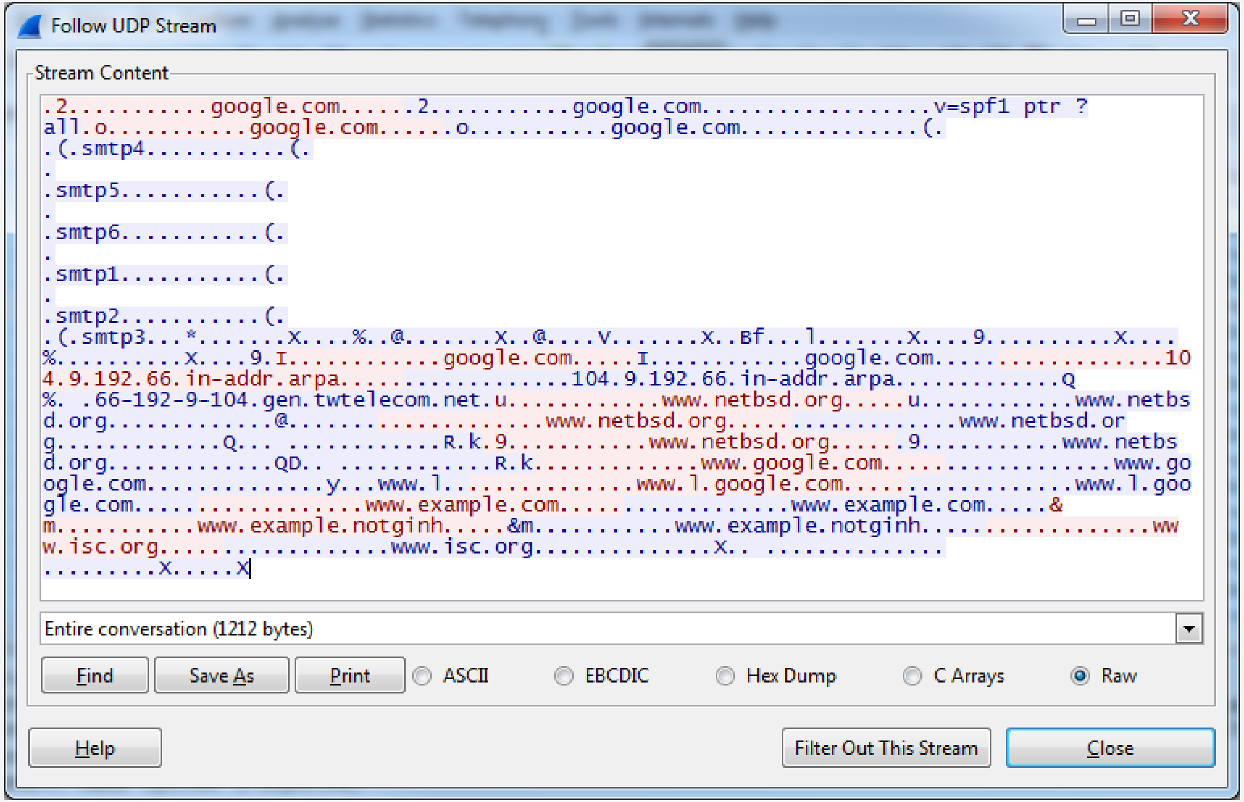
```
⊞ Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
⊞ Ethernet II, Src: AsustekC_b1:0c:ad (00:e0:18:b1:0c:ad), Dst: QuantaCo_32:41:8c (00:c0:9f:32:41:8c)
⊞ Internet Protocol Version 4, Src: 192.168.170.8 (192.168.170.8), Dst: 192.168.170.20 (192.168.170.20)
⊞ User Datagram Protocol, Src Port: 32795 (32795), Dst Port: domain (53)
⊞ Domain Name System (query)
```

DNS Resolution Analysis

» Viewing the stream

- Review entire conversation
- Look for anomalies in communication
- Look for false records
- Look for zone information

DNS Resolution Analysis



Stream Content

```
.2...........google.com......2...........google.com..................v=spf1 ptr ?
all.o...........google.com......o...........google.com..............(.
.(.smtp4...........(.
.
.smtp5...........(.
.
.smtp6...........(.
.
.smtp1...........(.
.
.smtp2...........(.
.(.smtp3...*.......x....%..@.......x..@....v.......x..Bf...l.......x....9..........x....
%..........x....9.I............google.com.....I............google.com..................10
4.9.192.66.in-addr.arpa..................104.9.192.66.in-addr.arpa.............Q
%. .66-192-9-104.gen.twtelecom.net.u............www.netbsd.org.....u............www.netbs
d.org.............@....................www.netbsd.org..................www.netbsd.or
g.............Q.. .............R.k.9...........www.netbsd.org......9...........www.netbs
d.org.............QD.. ............R.k.............www.google.com..................www.go
ogle.com..............y...www.l...............www.l.google.com..................www.l.goo
gle.com..................www.example.com..................www.example.com.....&
m...........www.example.notginh.....&m...........www.example.notginh..................ww
w.isc.org..................www.isc.org..............x.. ..............
.........x.....x
```

Entire conversation (1212 bytes)

Questions?