

AM.EN.P2CSN20020

1) Try to make different types (A,NS,MX) of DNS queries and map the response to the protocol structure

meas2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

[frame 88:19] == c0:0c:00:02:00:01:b3:59:00:07:01:62:02:6e:73:c0:0c

No.	Time	Source	Destination	Protocol	Length	Info
63...	103.3281...	192.168.0.1	192.168.0.106	DNS	331	Standard query response 0x121a A facebook.com A 31.13.79.35 NS b.ns.facebook.com NS c.ns.f...

> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 4
Additional RRs: 8

> Queries

- > facebook.com: type A, class IN

Type A

> Answers

- > facebook.com: type A, class IN, addr 31.13.79.35

> Authoritative nameservers

- > facebook.com: type NS, class IN, ns b.ns.facebook.com
- > facebook.com: type NS, class IN, ns c.ns.facebook.com
- > facebook.com: type NS, class IN, ns a.ns.facebook.com
- > facebook.com: type NS, class IN, ns d.ns.facebook.com

Type NS

> Additional records

- > a.ns.facebook.com: type A, class IN, addr 129.134.30.12
- > a.ns.facebook.com: type AAAA, class IN, addr 2a03:2880:f0fc:c:face:b00c:0:35
- > b.ns.facebook.com: type A, class IN, addr 129.134.31.12
- > b.ns.facebook.com: type AAAA, class IN, addr 2a03:2880:f0fd:c:face:b00c:0:35
- > c.ns.facebook.com: type A, class IN, addr 185.89.218.12
- > c.ns.facebook.com: type AAAA, class IN, addr 2a03:2880:f1fc:c:face:b00c:0:35
- > d.ns.facebook.com: type A, class IN, addr 185.89.219.12
- > d.ns.facebook.com: type AAAA, class IN, addr 2a03:2880:f1fd:c:face:b00c:0:35

[Request In: 6385]
[Time: 0.021033000 seconds]

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
74...	413.6481...	192.168.0.106	192.168.0.1	DNS	74	Standard query 0xfd55 A ogs.google.com
74...	413.6520...	192.168.0.1	192.168.0.106	DNS	359	Standard query response 0xfd55 A ogs.google.com CNAME www3.l.google.com A 172.217.27.206...
74...	414.0973...	192.168.0.106	192.168.0.1	DNS	75	Standard query 0xfb93 A ssl.gstatic.com
74...	414.0973...	192.168.0.106	192.168.0.1	DNS	75	Standard query 0x3b07 A www.gstatic.com
74...	414.0978...	192.168.0.106	192.168.0.1	DNS	75	Standard query 0x68e2 A apis.google.com
74...	414.1020...	192.168.0.1	192.168.0.106	DNS	346	Standard query response 0x3b07 A www.gstatic.com A 216.58.203.35 NS ns2.google.com NS ns...
74...	414.1021...	192.168.0.1	192.168.0.106	DNS	346	Standard query response 0xfb93 A ssl.gstatic.com A 142.250.67.227 NS ns2.google.com NS n...
74...	414.1030...	192.168.0.1	192.168.0.106	DNS	360	Standard query response 0x68e2 A apis.google.com CNAME plus.l.google.com A 216.58.196.78...
74...	414.6293...	192.168.0.106	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
74...	414.6361...	192.168.0.1	192.168.0.106	DNS	139	Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa SOA 168.192.IN-...
74...	414.6393...	192.168.0.106	192.168.0.1	DNS	69	Standard query 0x0002 MX gmail.com
74...	414.6431...	192.168.0.1	192.168.0.106	DNS	472	Standard query response 0x0002 MX gmail.com MX 10 alt1.gmail-smtp-in.l.google.com MX 30 ...
79...	473.3527...	192.168.0.106	192.168.0.1	DNS	76	Standard query 0xaf7f A web.whatsapp.com
79...	473.3591...	192.168.0.1	192.168.0.106	DNS	372	Standard query response 0xaf7f A web.whatsapp.com CNAME mmx-ds.cdn.whatsapp.net A 157.24...

> gmail.com: type MX, class IN
Name: gmail.com
[Name Length: 9]
[Label Count: 2]
Type: MX (Mail eXchange) (15)
Class: IN (0x0001)

> Answers

- > gmail.com: type MX, class IN, preference 10, mx alt1.gmail-smtp-in.l.google.com
- > gmail.com: type MX, class IN, preference 30, mx alt3.gmail-smtp-in.l.google.com
- > gmail.com: type MX, class IN, preference 20, mx alt2.gmail-smtp-in.l.google.com
- > gmail.com: type MX, class IN, preference 5, mx gmail-smtp-in.l.google.com
- > gmail.com: type MX, class IN, preference 40, mx alt4.gmail-smtp-in.l.google.com

> Authoritative nameservers

- > gmail.com: type NS, class IN, ns ns2.google.com

Type MX

Query Class (dns.qry.class), 2 bytes

Packets: 8188 · Displayed: 76 (0.9%)

Profile: Default

17:23
05-10-2020