

Aluno: Matheus Rambo da Roza

## Análise de tráfego no Wireshark.

ip.addr == 192.168.43.1						
No.	Time	Source	Destination	Protocol	Length	Info
162	19.355909	192.168.43.198	192.168.43.1	DNS	86	Standard query 0xad0d A cloudsearch.googleapis.com
163	19.357046	192.168.43.198	192.168.43.1	DNS	86	Standard query 0x3f93 AAAA cloudsearch.googleapis.com
164	19.444353	192.168.43.1	192.168.43.198	DNS	102	Standard query response 0xad0d A cloudsearch.googleapis.com A 172.217.173.74
165	19.453760	192.168.43.1	192.168.43.198	DNS	114	Standard query response 0x3f93 AAAA cloudsearch.googleapis.com AAAA 2800:3f0:4001:819::200a
287	20.886298	192.168.43.198	192.168.43.1	DNS	73	Standard query 0x5a10 A id.google.com
288	20.886770	192.168.43.198	192.168.43.1	DNS	73	Standard query 0xbde2 AAAA id.google.com
291	20.949507	192.168.43.1	192.168.43.198	DNS	89	Standard query response 0x5a10 A id.google.com A 172.217.29.227
292	20.949507	192.168.43.1	192.168.43.198	DNS	101	Standard query response 0xbde2 AAAA id.google.com AAAA 2800:3f0:4001:81b::2003
334	21.594681	192.168.43.198	192.168.43.1	DNS	87	Standard query 0xa939 A googleds.g.doubleclick.net
335	21.595293	192.168.43.198	192.168.43.1	DNS	87	Standard query 0x32f0 AAAA googleds.g.doubleclick.net
336	21.677510	192.168.43.1	192.168.43.198	DNS	128	Standard query response 0xa939 A googleds.g.doubleclick.net CNAME pagead46.l.doubleclick.net A 172.217.30...
337	21.685405	192.168.43.1	192.168.43.198	DNS	140	Standard query response 0x32f0 AAAA googleds.g.doubleclick.net CNAME pagead46.l.doubleclick.net AAAA 2800:...
352	21.878498	192.168.43.198	192.168.43.1	DNS	80	Standard query 0x4b8e A adservice.google.com
353	21.879322	192.168.43.198	192.168.43.1	DNS	80	Standard query 0xc10b AAAA adservice.google.com
363	21.967470	192.168.43.1	192.168.43.198	DNS	136	Standard query response 0x4b8e A adservice.google.com CNAME pagead46.l.doubleclick.net A 172.217.30.162
364	21.967470	192.168.43.1	192.168.43.198	DNS	148	Standard query response 0xc10b AAAA adservice.google.com CNAME pagead46.l.doubleclick.net AAAA 2800:3f0:400...
401	24.152089	192.168.43.198	192.168.43.1	DNS	88	Standard query 0xb64e AAAA fcmconnection.googleapis.com
402	24.274594	192.168.43.1	192.168.43.198	DNS	116	Standard query response 0xb64e AAAA fcmconnection.googleapis.com AAAA 2800:3f0:4001:81b::200a
438	26.631100	192.168.43.198	192.168.43.1	DNS	75	Standard query 0xd2b0 A ssl.gstatic.com

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 66

Identification: 0x4a54 (19028)

> Flags: 0x00

Fragment Offset: 0

Time to Live: 128

Protocol: UDP (17)

Header Checksum: 0x183f [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.43.198

Destination Address: 192.168.43.1

> User Datagram Protocol, Src Port: 52112, Dst Port: 53

> Domain Name System (query)

DNS sempre resolvendo os problemas de nomes. Podemos observar a conversa entre meu IP 192.168.43.1 e o IP do roteador do meu celular (Estava sem internet esse final de semana).

Pelo o que o wireshark capturou, houve uma conversa intensa entre meu note e o roteador do meu celular, não entendi o porque não saiu nenhum pacote para fora do meu roteador do celular. Pelo visto o meu roteador do celular “Resolveu” todo o problema. Ou foi porque eu coloquei o filtro de mostrar somente o que ocorria envolvendo meu IP, o que faz mais sentido.