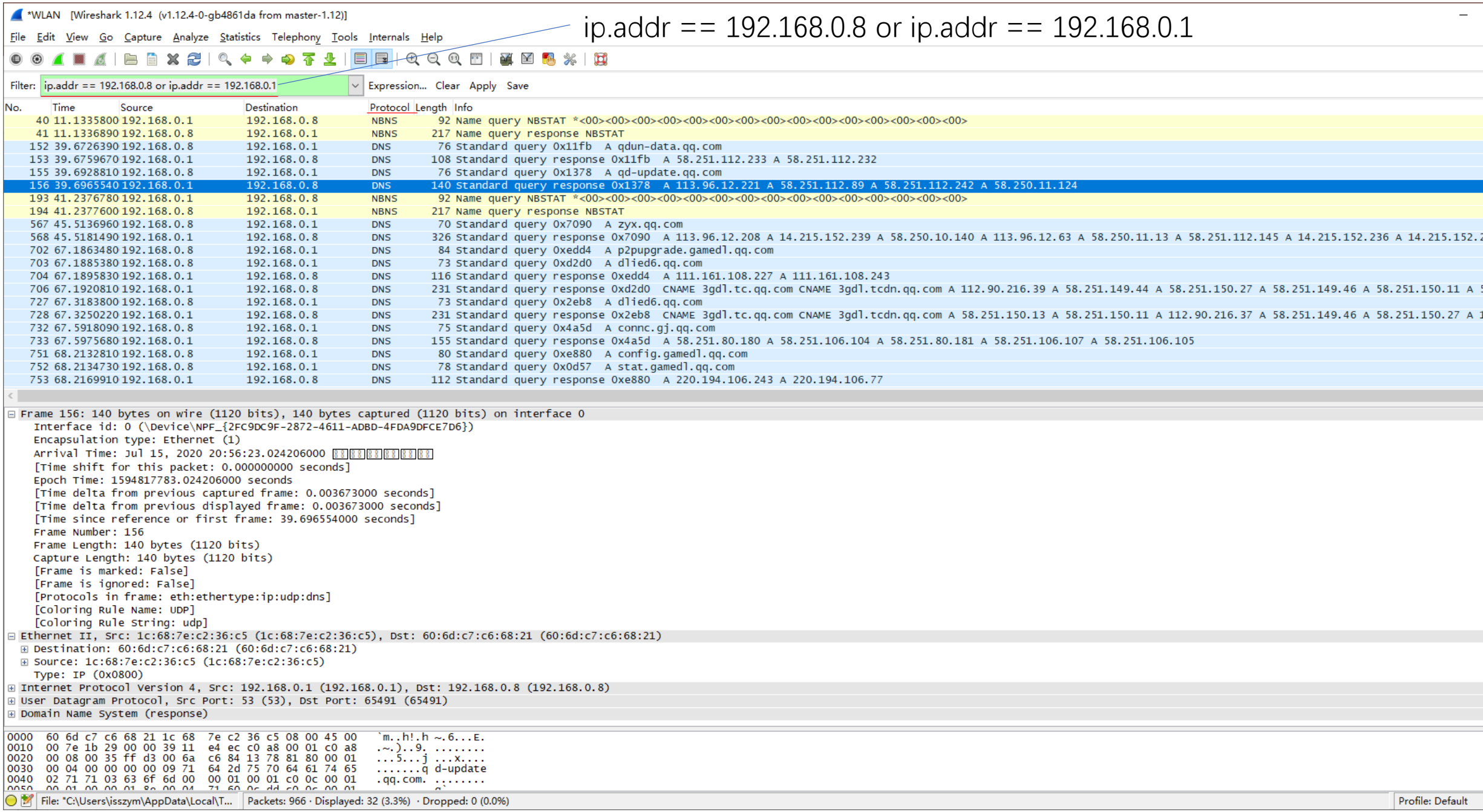
WireShark


*WLAN [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
ip.addr == 192.168.0.8 or ip.addr == 192.168.0.1
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ip.addr == 192.168.0.8 or ip.addr == 192.168.0.1
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
40 11.1335800 192.168.0.1 192.168.0.8 NBNS 92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
41 11.1336890 192.168.0.8 192.168.0.1 NBNS 217 Name query response NBSTAT
152 39.6726390 192.168.0.8 192.168.0.1 DNS 76 Standard query 0x11fb A qdun-data.qq.com
153 39.6759670 192.168.0.1 192.168.0.8 DNS 108 Standard query response 0x11fb A 58.251.112.233 A 58.251.112.232
155 39.6928810 192.168.0.8 192.168.0.1 DNS 76 Standard query 0x1378 A qd-update.qq.com
156 39.6965540 192.168.0.1 192.168.0.8 DNS 140 Standard query response 0x1378 A 113.96.12.221 A 58.251.112.89 A 58.251.112.242 A 58.250.11.124
193 41.2376780 192.168.0.1 192.168.0.8 NBNS 92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
194 41.2377600 192.168.0.8 192.168.0.1 NBNS 217 Name query response NBSTAT
567 45.5136960 192.168.0.8 192.168.0.1 DNS 70 Standard query 0x7090 A zyx.qq.com
568 45.5181490 192.168.0.1 192.168.0.8 DNS 326 Standard query response 0x7090 A 113.96.12.208 A 14.215.152.239 A 58.250.10.140 A 113.96.12.63 A 58.250.11.13 A 58.251.112.145 A 14.215.152.236 A 14.215.152.2
702 67.1863480 192.168.0.8 192.168.0.1 DNS 84 Standard query 0xedd4 A p2pupgrade.gamedl.qq.com
703 67.1885380 192.168.0.8 192.168.0.1 DNS 73 Standard query 0xd2d0 A dlied6.qq.com
704 67.1895830 192.168.0.1 192.168.0.8 DNS 116 Standard query response 0xedd4 A 111.161.108.227 A 111.161.108.243
706 67.1920810 192.168.0.1 192.168.0.8 DNS 231 Standard query response 0xd2d0 CNAME 3gdl.tc.qq.com CNAME 3gdl.tcdn.qq.com A 112.90.216.39 A 58.251.149.44 A 58.251.150.27 A 58.251.149.46 A 58.251.150.11 A 5
727 67.3183800 192.168.0.8 192.168.0.1 DNS 73 Standard query 0x2eb8 A dlied6.qq.com
728 67.3250220 192.168.0.1 192.168.0.8 DNS 231 Standard query response 0x2eb8 CNAME 3gdl.tc.qq.com CNAME 3gdl.tcdn.qq.com A 58.251.150.13 A 58.251.150.11 A 112.90.216.37 A 58.251.149.46 A 58.251.150.27 A 1
732 67.5918090 192.168.0.8 192.168.0.1 DNS 75 Standard query 0x4a5d A connc.gj.qq.com
733 67.5975680 192.168.0.1 192.168.0.8 DNS 155 Standard query response 0x4a5d A 58.251.80.180 A 58.251.106.104 A 58.251.80.181 A 58.251.106.107 A 58.251.106.105
751 68.2132810 192.168.0.8 192.168.0.1 DNS 80 Standard query 0xe880 A config.gamedl.qq.com
752 68.2134730 192.168.0.8 192.168.0.1 DNS 78 Standard query 0x0d57 A stat.gamedl.qq.com
753 68.2169910 192.168.0.1 192.168.0.8 DNS 112 Standard query response 0xe880 A 220.194.106.243 A 220.194.106.77
Frame 156: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Interface id: 0 (\Device\NPF_{2FC9DC9F-2872-4611-ADBD-4FDA9DFCE7D6})
Encapsulation type: Ethernet (1)
Arrival Time: Jul 15, 2020 20:56:23.024206000
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1594817783.024206000 seconds
[Time delta from previous captured frame: 0.003673000 seconds]
[Time delta from previous displayed frame: 0.003673000 seconds]
[Time since reference or first frame: 39.696554000 seconds]
Frame Number: 156
Frame Length: 140 bytes (1120 bits)
Capture Length: 140 bytes (1120 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: 1c:68:7e:c2:36:c5 (1c:68:7e:c2:36:c5), Dst: 60:6d:c7:c6:68:21 (60:6d:c7:c6:68:21)
Destination: 60:6d:c7:c6:68:21 (60:6d:c7:c6:68:21)
Source: 1c:68:7e:c2:36:c5 (1c:68:7e:c2:36:c5)
Type: IP (0x0800)
Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.8 (192.168.0.8)
User Datagram Protocol, Src Port: 53 (53), Dst Port: 65491 (65491)
Domain Name System (response)
0000 60 6d c7 c6 68 21 1c 68 7e c2 36 c5 08 00 45 00 `m..h!.h ~.6...E.
0010 00 7e 1b 29 00 00 39 11 e4 ec c0 a8 00 01 c0 a8 .~.)..9. ....
0020 00 08 00 35 ff d3 00 6a c6 84 13 78 81 80 00 01 ...5...j ...x....
0030 00 04 00 00 00 00 09 71 64 2d 75 70 64 61 74 65 ....q d-update
0040 02 71 71 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 .qq.com. ....
File: "C:\Users\isszym\AppData\Local\T...
Packets: 966 · Displayed: 32 (3.3%) · Dropped: 0 (0.0%)
Profile: Default

ip.src==192.16.22.48 and ip.dst eq 192.16.22.1

tcp.port==9000 or udp.dstport==9000

eth.addr==00:11:22:33:44:55 and eth.src!=00:11:22:33:44:66

tcp.window_size < 1460

ip.ttl <= 10

http contains “GET” http.request.method=="GET"

udp.length==20 frame.len==20 ip.len==20

tcp.flags.syn==1

!arp 或者 not arp

协议：tcp udp arp icmp http smtp ftp dns ip ssl oicq bootp

lt < le <= eq = gt > ge >= ne !=

contains

and &&

or ||

任务

- IP Option（记录4个IP地址和记录4个地址时间戳）
- ICMP（Echo请求和Echo响应 ）
- TraceRT (ICMP请求TTL=1~4和TTL=0)
- ARP请求和响应
- DHCP--Discover、Offer、Request、Ack
- DNS请求和响应
- HTTP请求和响应