

Oleh: Indri Ristika Utami

The screenshot displays the Wireshark network protocol analyzer interface. The top pane shows a list of 16 captured packets, all of which are DNS queries and responses between the source IP 192.168.138.158 and the destination IP 192.168.138.2. The middle pane provides a detailed view of the selected packet (No. 137), showing the Ethernet II header, the Internet Protocol Version 4 header, the User Datagram Protocol header, and the Domain Name System (query) payload. The bottom pane displays the raw packet data in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.138.158	192.168.138.2	DNS	137	Standard query 0x47ae va872g.g90e1h.b8.642b63u.9j85a2.v33e.37.pa269cc.e8mfzdgfrf7g0.groupprograms.in
2	0.150951	192.168.138.2	192.168.138.158	DNS	153	Standard query response 0x47ae va872g.g90e1h.b8.642b63u.9j85a2.v33e.37.pa269cc.e8mfzdgfrf7g0.groupprograms.in
3	0.788952	192.168.138.158	192.168.138.2	DNS	136	Standard query 0x6a70 ubb67.3c1470.u080a4.w07d919.o5f.fl.b08w.r0faf9.e8mfzdgfrf7g0.groupprograms.in
4	0.789994	192.168.138.158	192.168.138.2	DNS	135	Standard query 0xf2bb r03afid.c3000e.x0807r.b0f.a39.h7f0fa5eu.vb0fb1.e8mfzdgfrf7g0.groupprograms.in
5	0.932551	192.168.138.2	192.168.138.158	DNS	152	Standard query response 0x6a70 a ubb67.3c1470.u080a4.w07d919.o5f.fl.b08w.r0faf9.e8mfzdgfrf7g0.groupprograms.in
6	0.946469	192.168.138.2	192.168.138.158	DNS	151	Standard query response 0xf2bb a r03afid.c3000e.x0807r.b0f.a39.h7f0fa5eu.vb0fb1.e8mfzdgfrf7g0.groupprograms.in
7	5.913981	192.168.138.158	192.168.138.2	DNS	70	Standard query 0x3cc1 a ip-addr.es
8	6.054761	192.168.138.2	192.168.138.158	DNS	86	Standard query response 0x3cc1 a ip-addr.es a 188.165.164.184
9	6.328996	192.168.138.158	192.168.138.2	DNS	70	Standard query 0x5c49 a runlove.us
10	6.366567	192.168.138.2	192.168.138.158	DNS	86	Standard query response 0x5c49 a runlove.us a 204.152.254.221
11	6.566440	192.168.138.158	192.168.138.2	DNS	89	Standard query 0x17c8 a kritischerkonsum.uni-koeln.de
12	6.750822	192.168.138.2	192.168.138.158	DNS	145	Standard query response 0x17c8 a kritischerkonsum.uni-koeln.de SOA noc2.rnz.uni-koeln.de
13	6.752041	192.168.138.158	192.168.138.2	DNS	78	Standard query 0xa275 a comarksecurity.com
14	6.784508	192.168.138.2	192.168.138.158	DNS	94	Standard query response 0xa275 a comarksecurity.com a 72.34.49.86
15	6.440897	192.168.138.158	192.168.138.2	DNS	91	Standard query 0x16b2 a 70qnsnzwm6zb7y.gigapaysun.com
16	6.440729	192.168.138.2	192.168.138.158	DNS	107	Standard query response 0x16b2 a 70qnsnzwm6zb7y.gigapaysun.com a 95.163.121.204

Frame 1: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface 0
 Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
 Internet Protocol Version 4, Src: 192.168.138.158, Dst: 192.168.138.2
 User Datagram Protocol, Src Port: 60078, Dst Port: 53
 Domain Name System (query)

1. Diberikan file pcap dan jawab pertanyaan di bawahnya:
 - a. Jelaskan secara detil tentang apa saja yang ada / terjadi dengan merujuk ke file terlampir.

Terdapat tiga bagian utama dari file yaitu packet list (bagian atas), packet details (bagian kiri bawah), dan packet bytes (bagian kanan bawah). File ini menggunakan protocol DNS dan protocol transportnya UDP dalam proses kirim mengirim yang melibatkan dua IP yaitu 192.168.138.158 ke 192.168.138.2 yang dapat dikonfirmasi dari info yang tersedia yaitu standard query dan standard query response. Dalam proses pengiriman, file ditangkap secara utuh tanpa ada potongan dengan jenis jaringan LAN dan TTL nya 128 menunjukkan bahwa system operasinya berupa Windows. Tetapi, terdapat keanehan pada file dimana alamat MAC kosong. Selain itu, domain terlalu panjang dan terlihat mencurigakan.

- b. Apakah file di tersebut ada hubungannya dengan keamanan informasi? Jika ya, jelaskan secara detail.

Dari informasi, terdapat domain yang panjang dan mencurigakan. Pola dari domain ini sangat mirip domain-domain yang diproduksi oleh DGA. Dilihat dari respon server, sebenarnya domain panjang lumrah digunakan di proses transaksi file ini, tetapi terdapat beberapa domain yang mencurigakan. Jika kita melihat query domain dari nomor 1,3, dan 5 dan coba dibandingkan dengan domain yang dengan pola dan panjang yang wajar seperti 7, 9, dan 11. Hal ini dikatakan mencurigakan karena domain 1, 3, dan 5 terlalu panjang dan tidak familiar dan jika kita melihat pada permintaan DNS berulang kali dalam interval waktu yang sangat singkat sepertinya manusia tidak dapat mengetik domain secara berulang kali dengan sangat cepat sehingga ini menunjukan seperti pola serangan DGA. Langkah selanjutnya yang dapat diambil adalah

memblokir domain mencurigakan tadi dan gunakan antivirus atau endpoint security untuk memeriksa adanya serangan malware.