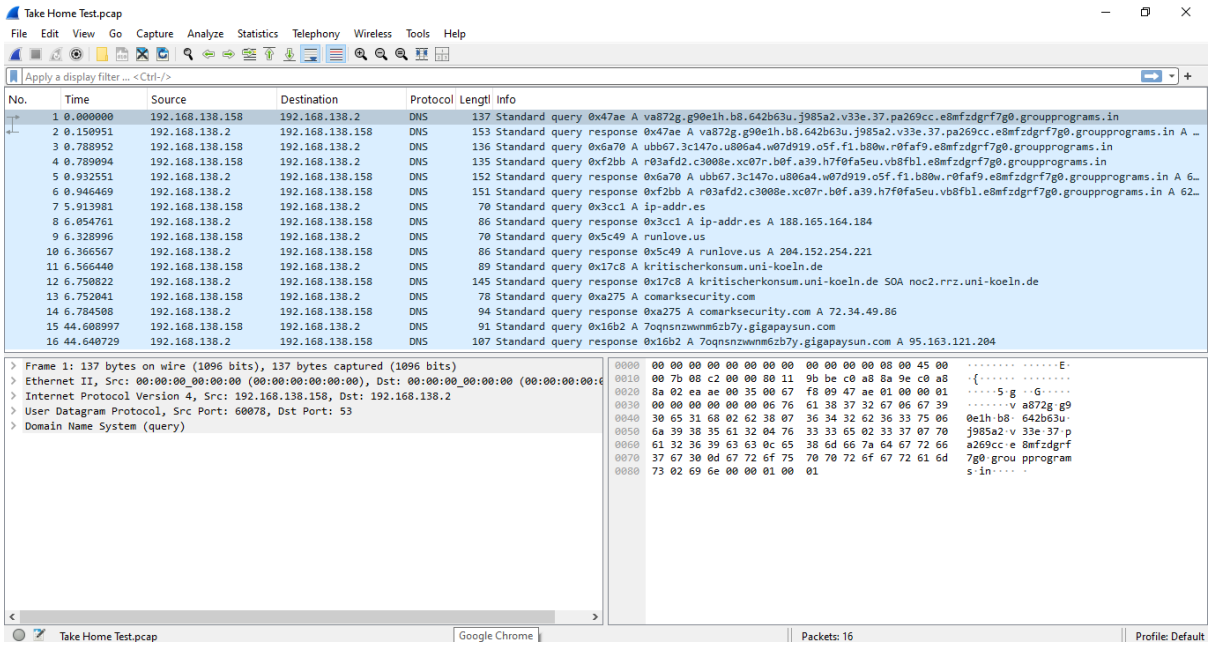
Analisis Jaringan

Oleh: Indri Ristika Utami



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 menunjukan 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 detil.

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 bandingkan 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 menujukan 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.