Executive Summary
DNS Traffic Analysis – Wireshark Investigation

A network packet capture containing 53,944 packets was analyzed using Wireshark to identify potential malicious DNS activity. The investigation focused on detecting DNS tunneling, Domain Generation Algorithm (DGA) behavior, beaconing activity, abnormal DNS resolution failures, and rogue DNS server usage.

The client system (172.17.84.79) communicated exclusively with the internal DNS resolver (172.17.80.1) over standard port 53. Long domain name analysis did not reveal high-entropy or encoded subdomains typically associated with DNS tunneling. Observed long domains were structured and linked to legitimate vendor infrastructure such as advertising and analytics services.

DNS error analysis revealed limited NXDOMAIN and SERVFAIL responses, consistent with standard browsing behavior. No excessive failure rate or repetitive random domain queries were detected, eliminating indicators of DGA-based malware.

UDP conversation analysis confirmed that each DNS transaction consisted of a single query and corresponding response. No repeated retry patterns, large payload anomalies, or sustained abnormal traffic volumes were observed.

Time-based I/O graph analysis showed traffic bursts correlated with manual browsing activity. No periodic or fixed-interval communication patterns indicative of beaconing were detected.

Conclusion:
The analyzed traffic represents normal baseline web browsing and background system activity. No indicators of compromise were identified.