Wireshark packet analysis: HTTP and DNS

Introduction

This assignment deals with analysing HTTP and DNS network traffic using wireshark. Be sure to read the submission guidelines for the assignment and remember the rules applicable to all assignments.

Question 1: HTTP packet analysis

Use the HTTP packet capture provided to answer the following questions.

1. What is the IP address of the client?
2. What is the IP address of the server?
3. What is the port number used by the client to communicate with the server?
4. What is the port number used by the server to communicate with the client?
5. What is the client identification string included in the HTTP messages?
6. What is the server identification string included in the HTTP messages?
7. What is the SHA256 hash of the HTML file transferred?
8. What is the ETag of the HTML file transferred?
9. What is the SHA256 hash of the other HTTP object transferred?
10. What is the ETag of other HTTP object transferred?

Question 2: DNS packet analysis

Use the DNS packet capture provided to answer the following questions.

1. What is the IP address of client performing the DNS resolution?
2. What is the IP address of the DNS server?
3. List all domains queried and type of DNS record requested by the client. Answer should be a JSON dictionary with keys as domains and values as record types.
4. List types of all responses received for domains queried by the client. Answer should be a JSON dictionary with keys as domains and values as JSON list of all record types received(even if only 1 response is received.)
5. List all IPs returned in all A records from the DNS server. Answer should be a JSON list.
6. List all domains returned in CNAME responses received from DNS server. Answer should be a JSON list.
7. List all domains returned in MX responses received from DNS server. Answer should be a JSON list.