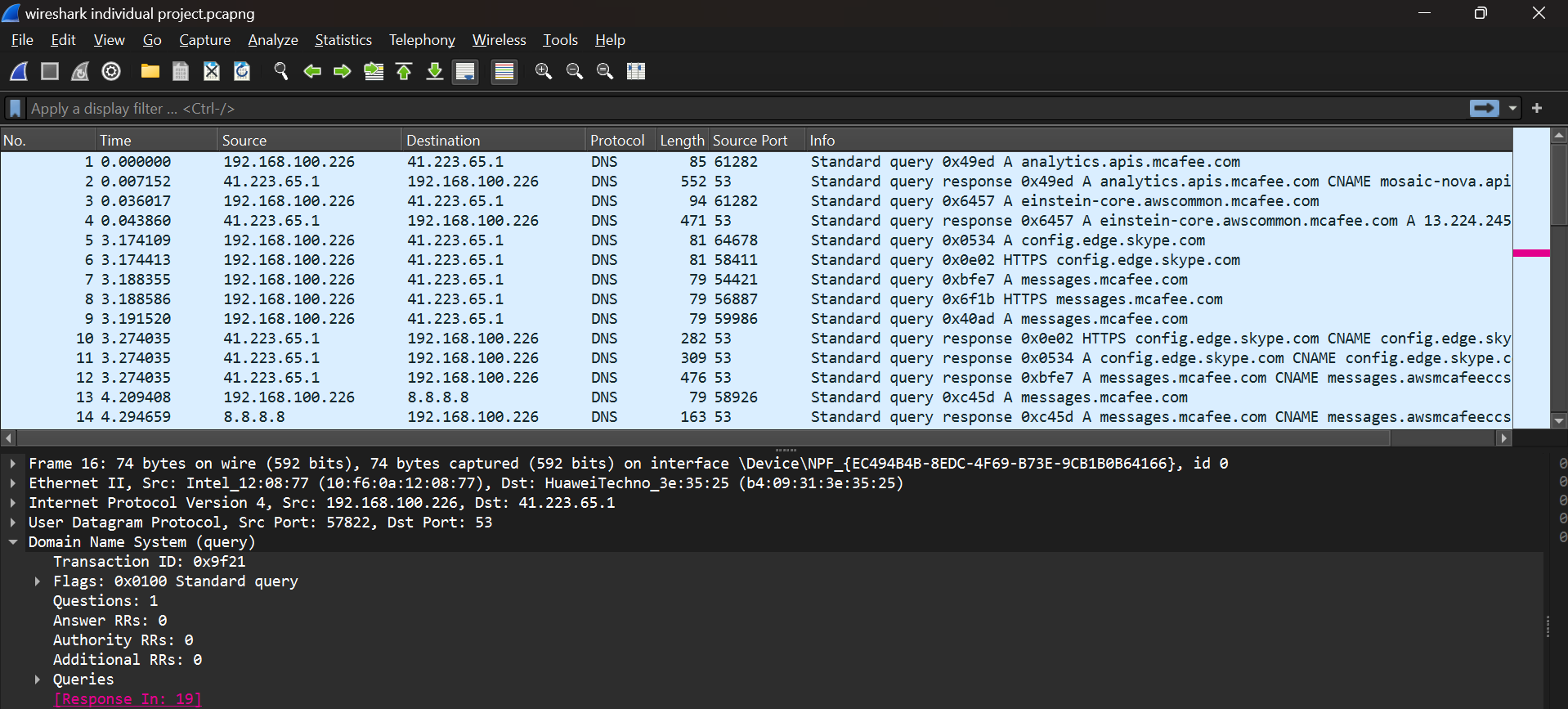
**CHISOROM OBIKA**

**NETWORK ANALYSIS OF DNS TRAFFIC USING WIRESHARK**



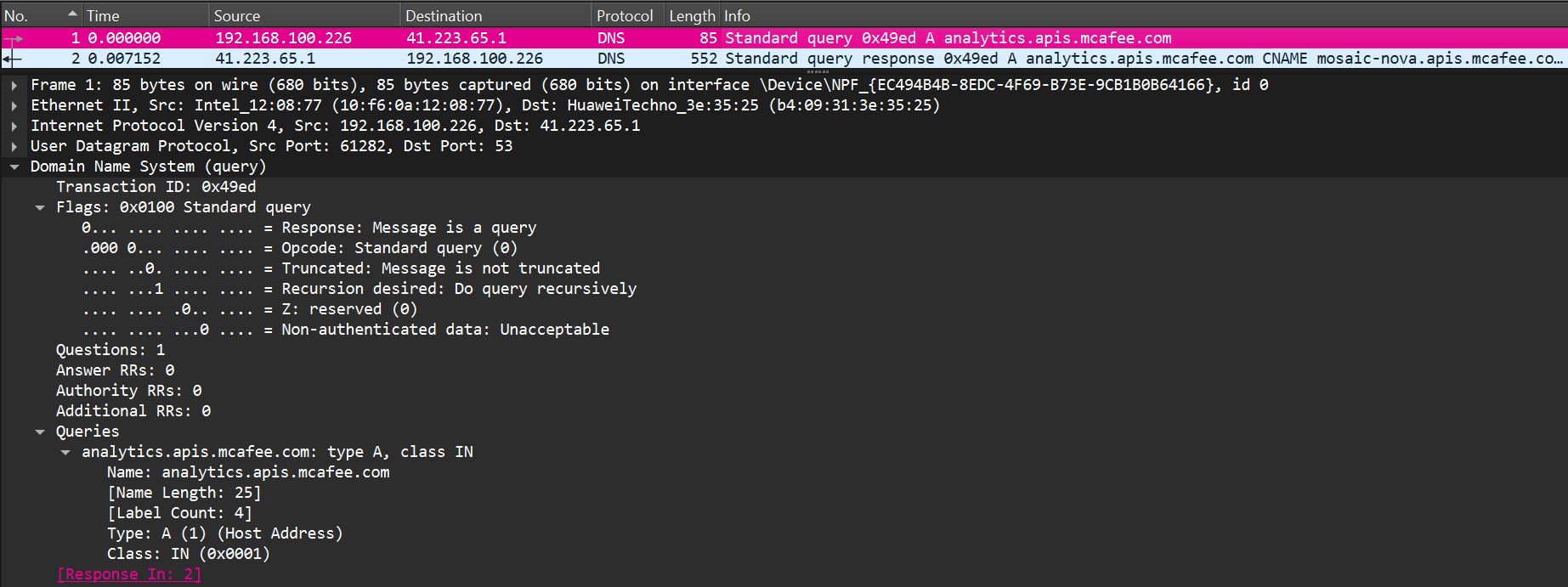
***Full Wireshark Screenshot of DNS network traffic***

**OVERVIEW OF DOMAIN NAMES AND THEIR IP ADDRESSES**

The port 53 Capture filter was used at the start of this Wireshark capture to ensure only DNS traffic was gotten. From the IP address column of the captured traffic, we can determine that the communication takes place between 3 main IP addresses. That is, IP address 192.168.100.226 which belongs to the host device querying the domain name **mcafee.com.** The IP address 41.223.65.1, which is the address of the domain name. Lastly, we have the IP address 8.8.8.8. It is the public domain name service run by Google and used for resolving domain names to IP addresses.

**Analysis of DNS query and query responses based on transaction ID pairs.**

The first 2 packets of the capture will be examined as they both have the same transaction ID **0x49ed.**



On the first line, the source IP address 192.168.100.226 sends a query to a DNS server asking for the IP address of  **analytics.apis.mcafee.com** which has been given as 41.223.65.1

**Interpreting results of the query message**

**Flags section:** Under this section, **Response** 0 identifies the message is a query. The Opcode with 4 0’s or 4 bits shows it is a standard DNS query. **Truncated** simply means that the character limit for the column was exceeded and therefore cut off. In this case, it shows the query message is not truncated. **Recursion desired: do query recursively** is 1 and this shows that the server will look for the domain name on behalf of the client and will ask other servers if it does not know the answer to the query.

**Questions section**: This shows that the host is asking only 1 question. A question asking for the IP address of analytics.apis.mcafee.com

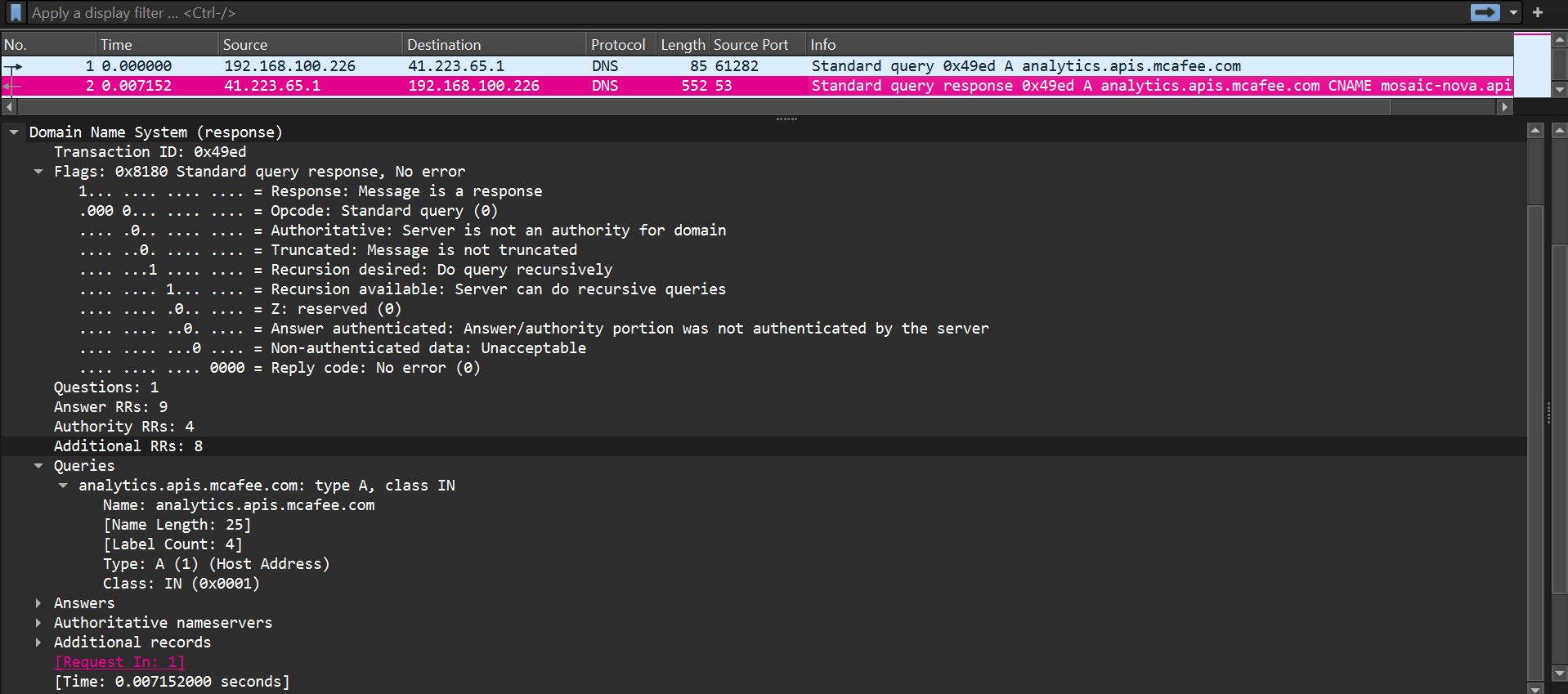
**Answer RRs/Authority RRs/Additional RRs:** These are all 0 because it is a query and therefore has only questions and no answers.

**Name:** This is the requested domain name

Lastly, **Type A** in the queries section shows that it is an IPV4 address.

**Interpreting results of the query response message**

In this section, the corresponding query response message will be analyzed.

****

**Flags section:** Under the flags section, **Response** 1 identifies that the message is a response to a query.

**Questions section:** This shows that the host is asking only 1 question. A question asking for the IP address of analytics.apis.mcafee.com.

**Answer RRs/Authority RRs/Additional RRs:** Here we have 9, 4 and 8 responses respectively as it is a query response message.

**Conclusion**

A proper response was given to the query. Therefore there are no DNS-related issues.