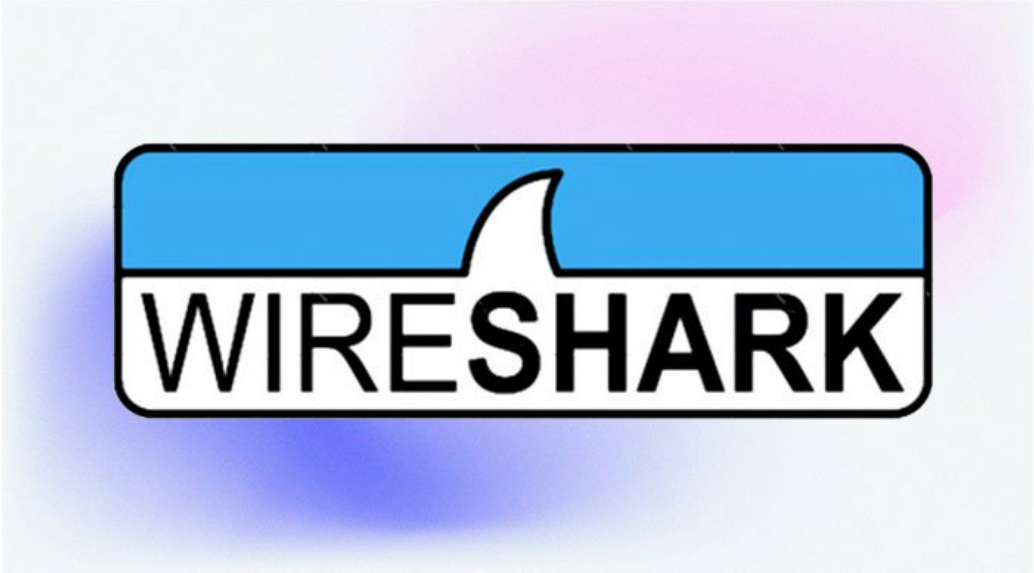
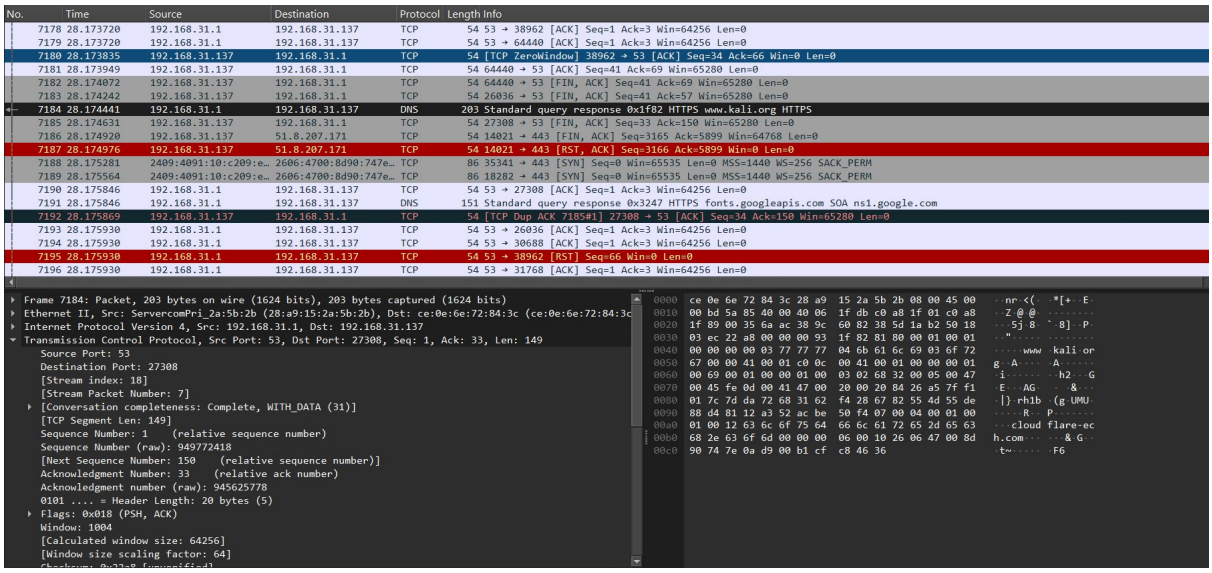
Capture and Analyze Network Traffic Using Wireshark.



- **Installation Wireshark and use Wireshark to find DNS Traffics.**

- **Starting Capture on Your Active Network Interface**

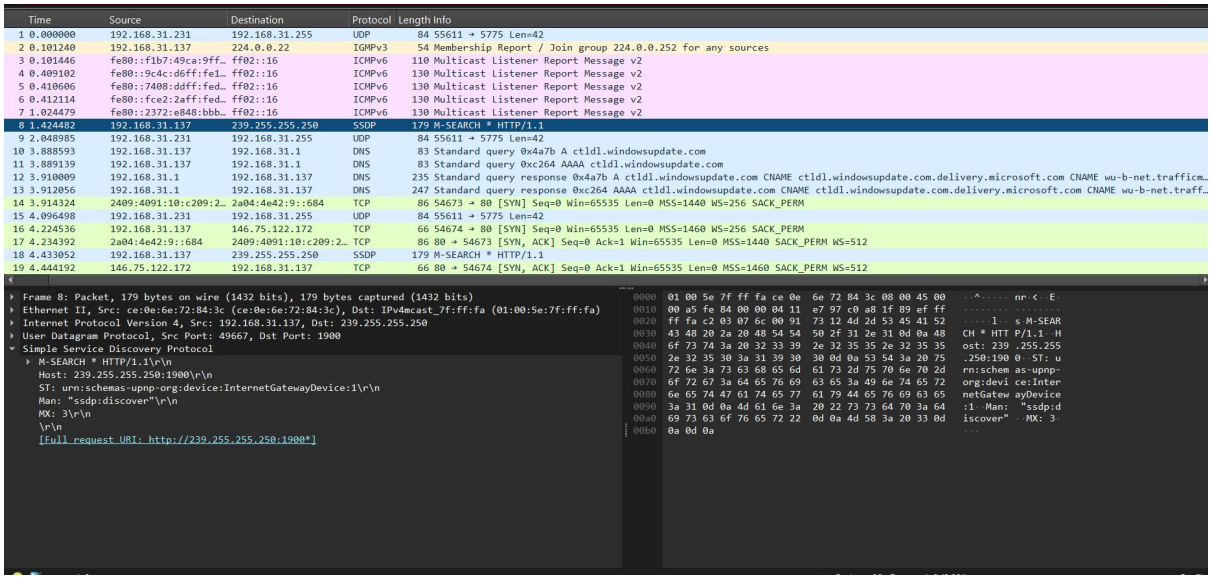
Sample : https://www.kali.org/ (for Https)

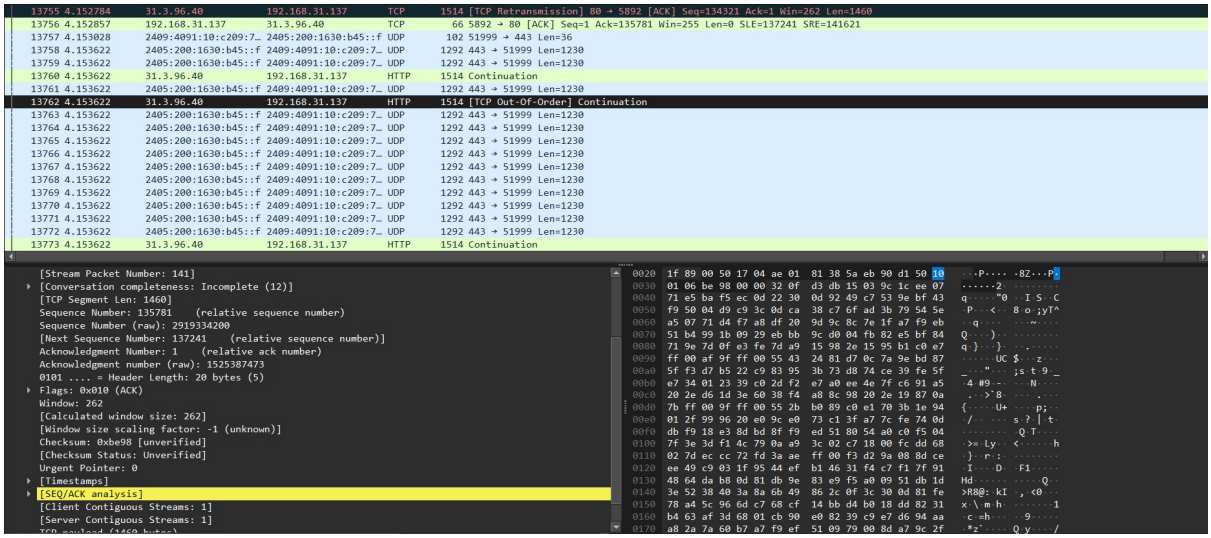


Using wireshark and found this type result :

Here DNS Traffic and HTTPS traffic reports

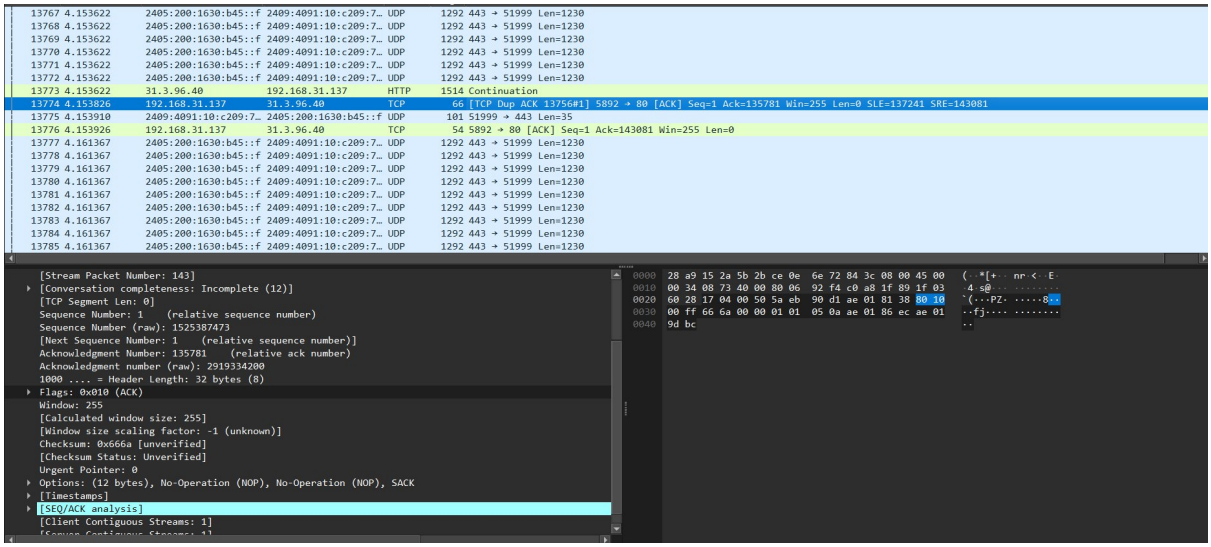
And the second time we found the HTTP traffic report : (Random)





Here we find two types of HTTP report randomly.

Here We found the TCP traffic report:



Here In Wireshark, ACK stands for acknowledgment and signifies that a TCP packet was received successfully. When the ACK flag is set, it tells the receiving host to process the acknowledgment number in the packet, which confirms the receipt of data from the other side of the connection. This flag is fundamental to TCP's reliability, ensuring that data is delivered correctly and coordinating the flow of information.

- **Confirmation of receipt:**

An ACK packet is sent in response to a data packet to confirm that it was received by the destination.

- **Coordination of data flow:**

It is a key part of the TCP handshake, which establishes and maintains a reliable connection by coordinating the flow of data between two hosts.

- **Used with other flags:**

You will often see ACK used with other flags, such as SYN, ACK (used to establish a connection) or FIN, ACK (used to gracefully close a connection).

- **Reliability:**

Without the ACK flag, there would be no reliable way for a host to confirm that the data it sent was successfully received by the other party.

Here is the result of wireshark packet traffic like DNS, HTTP, TCP packet Traffic sniffing.

Thankyou.