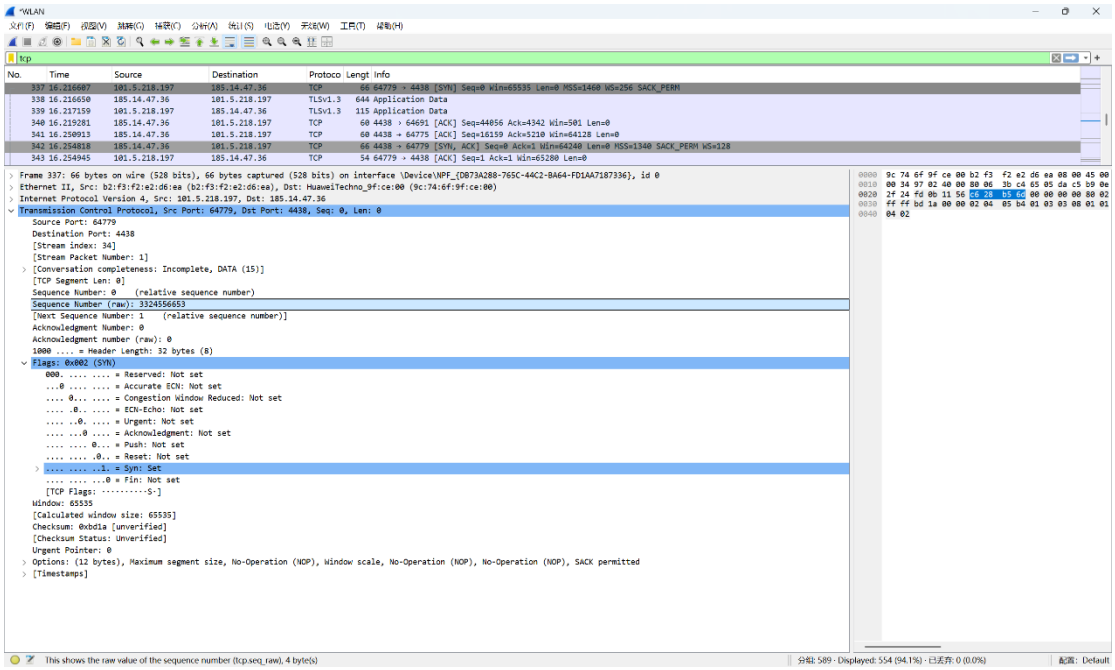
# Wireshark


## Zhong Jiaxuan, CS class 35, 2023010812

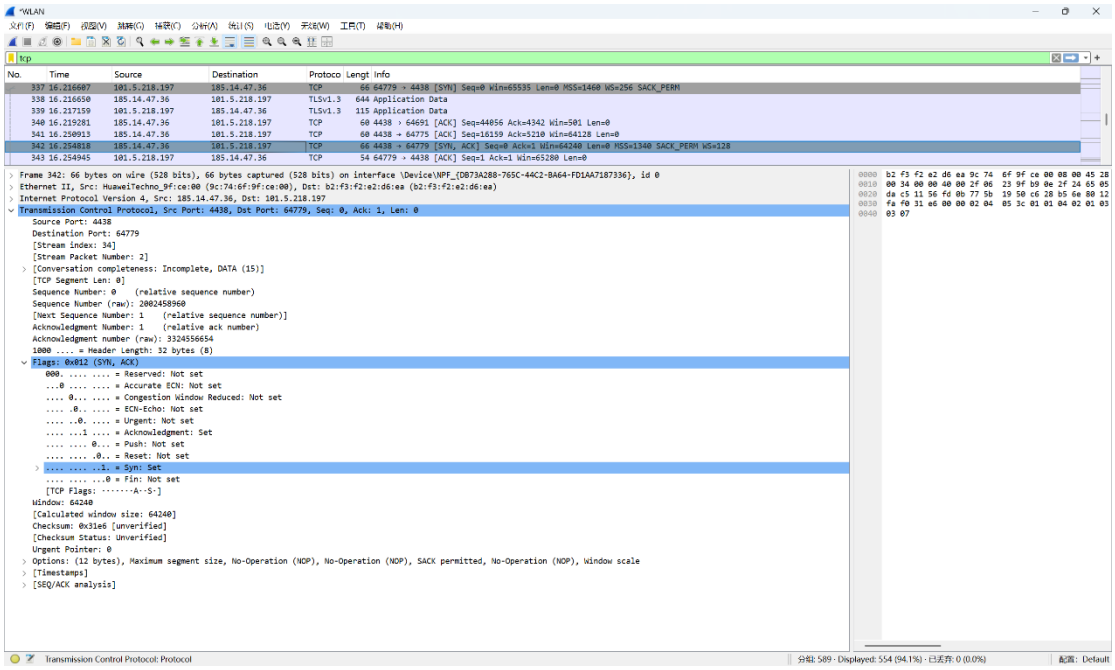

# TCP

**Generally, TCP three-way handshake are like this:**

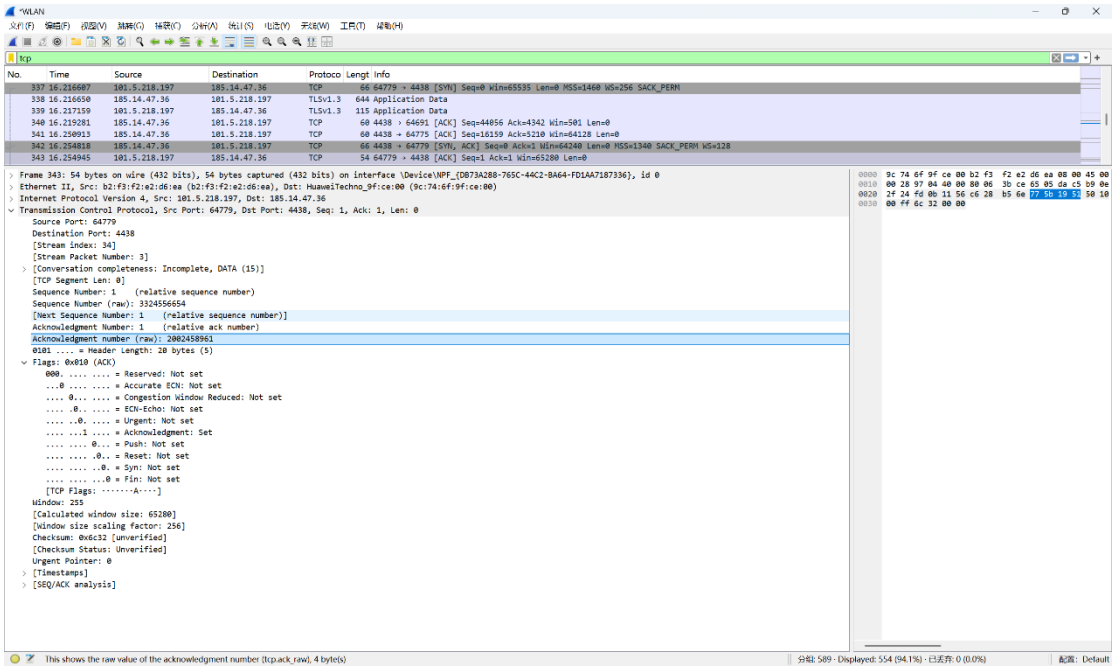
**First.** Client send SYN to Server, require to establish connection. SYN packet has its Src a physical address and its Dst `HuaweiTechno_9f:ce:00`, which might be the router of Tsinghua or somewhere of the Internet infrastructure. Also, the SYN packets set its flag `Syn`, but not `Acknowledgement`.




**Second.** Server send back SYN+ACK, accept the require of Client and require back. We can see the swap of Src and Dst, and the flags have its `Syn` and `Acknowledgement` set.




**Third.** Client send ACK to Server, accept the require-back. The Src and Dst swap again and only `Acknowledgement` flag is set.



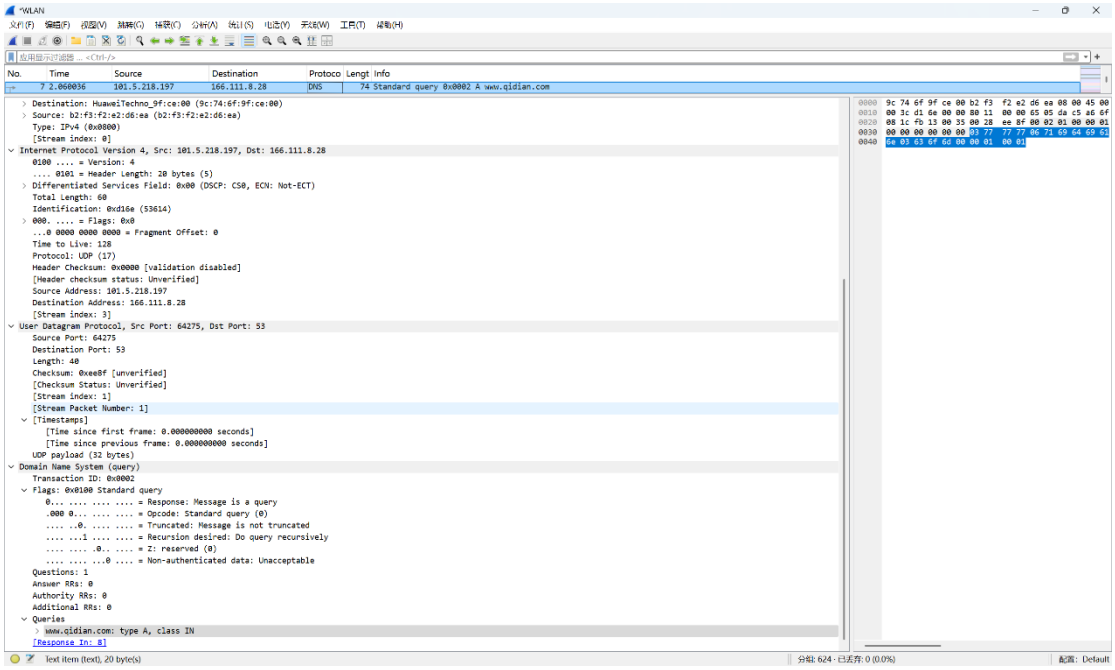

It has two big random numbers as raw `Sequence Number`(or `Seq`) and `Acknowledgement Number`(or `Ack`), and use the offset as true such numbers. `Seq` is indeed "The packet I am sending now" while `Ack` is "Which your packet I want".

`Seq` increases only because the counterpart has its `Ack` increased.

The place of `Seq` and `Ack` are highlighted in the 1st and 3rd pictures.

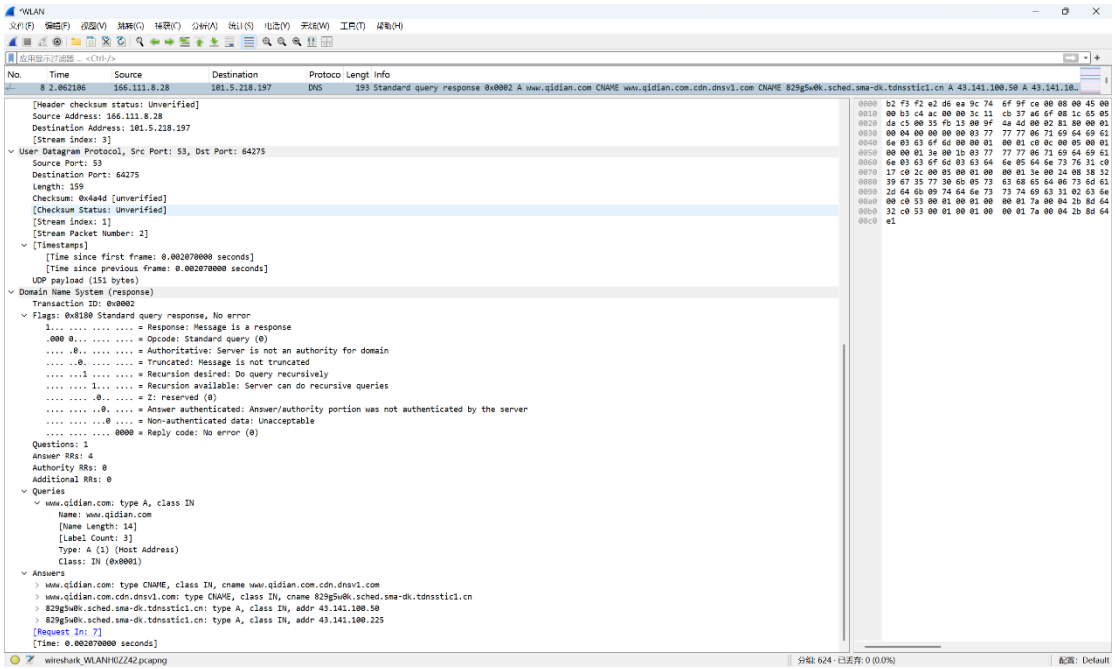
# DNS

## DNS request:




We have Src IP 101.5.218.197 and Dst IP 166.111.8.28 same as the prior TCP Dst, maybe this is the Server of THU.

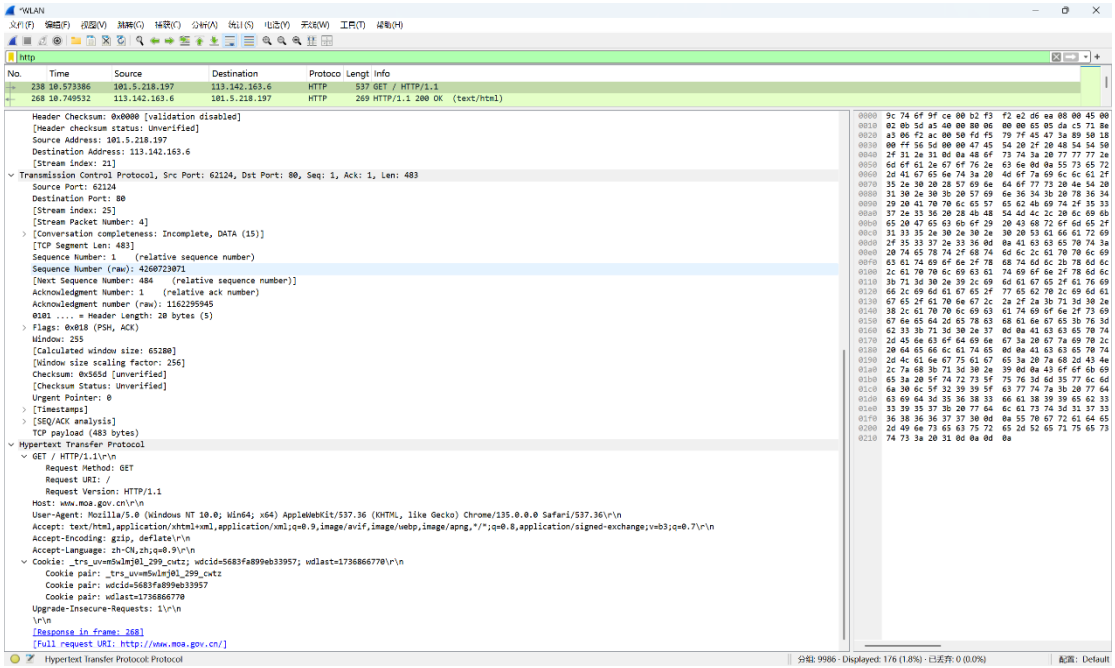
## DNS respond:




We send a type A query in No.7 packet, but return 4 queries in No.8 packet. It shows that `www.qidian.com` has a cname `www.qidian.com.cdn.dnsv1.com`, and the latter has a cname `829g5w0k.sched.sma-dk.tdnsstic1.cn`, and then 2 type A answer, the complex cname has 2 IPs `43.141.100.50` and `43.141.100.225`.

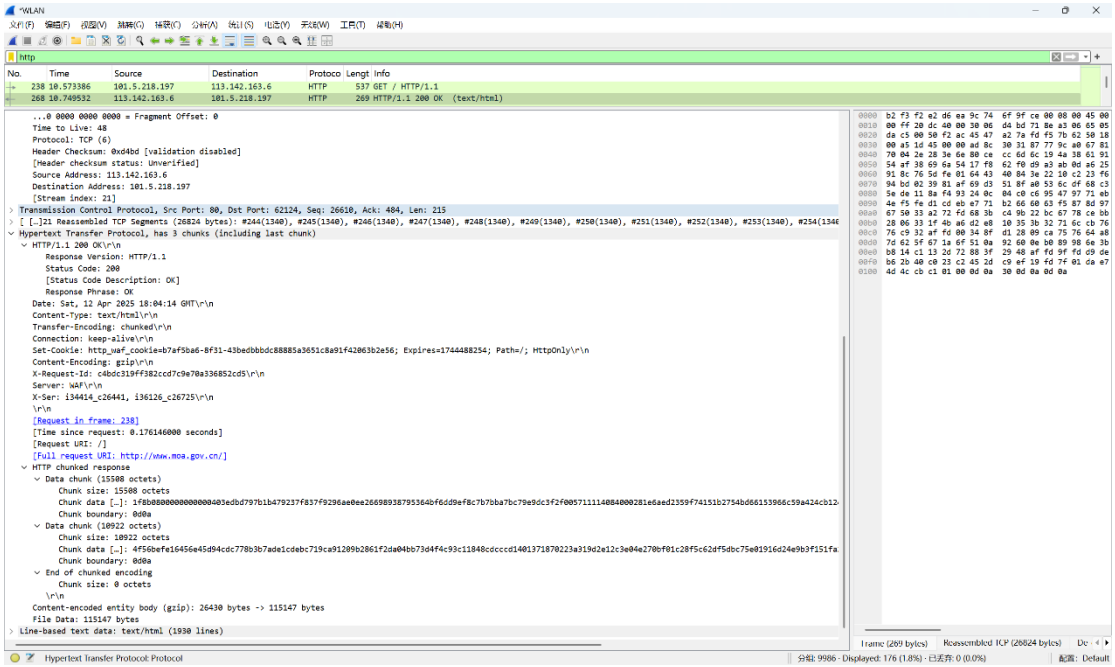
# HTTP

## HTTP request:



We have a HTTP request with method `GET` at the head of `Hypertext Transfer Protocol`. Type of required answers are in `Accept`, like `text/html`.

## HTTP answer:



The status code is in `HTTP/1.1 200 OK\r\n`, the `200 OK`, and the `Content-type` responds to the `Accept` of the request.