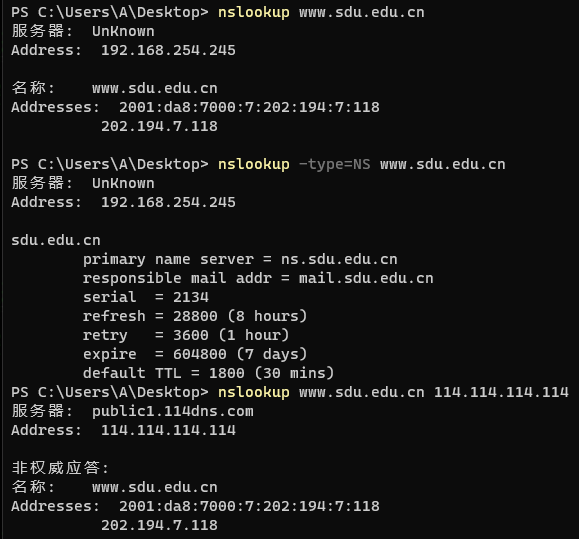
Wireshark Lab 7-1

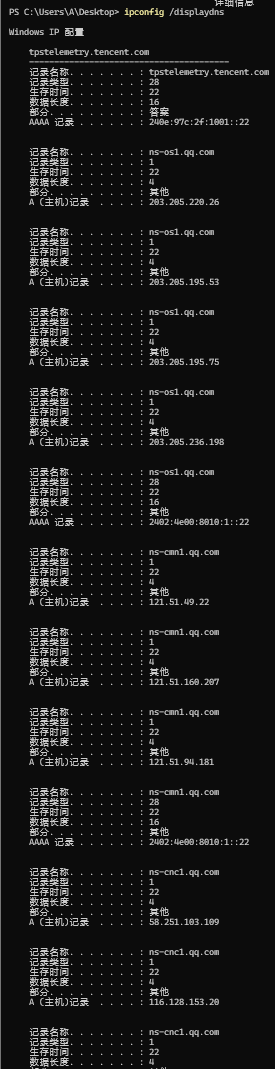
202022300317 杨业昶

## 1: nslookup

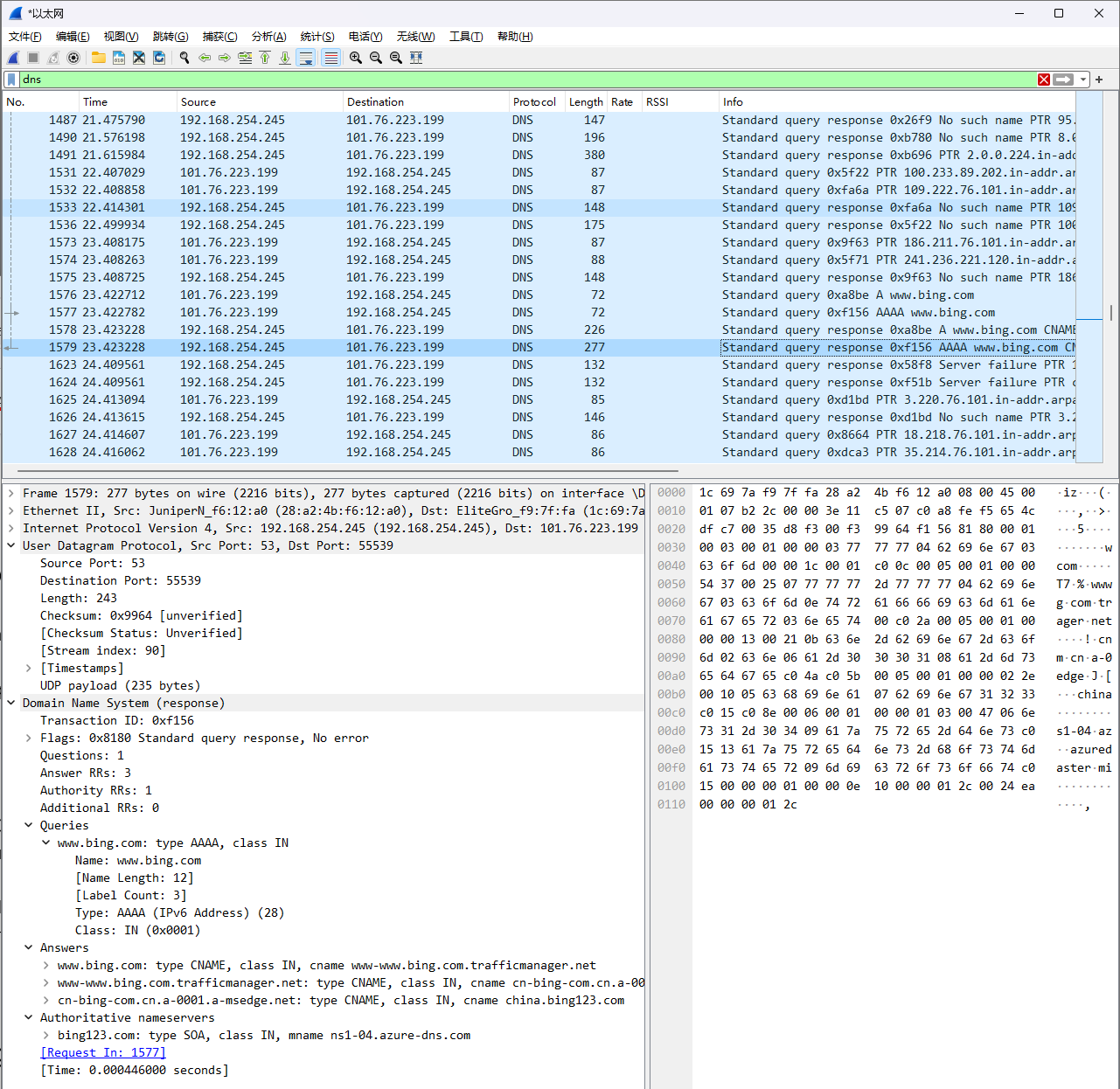


## 2: ipconfig





## 3: Tracing DNS with Wireshark



Locate the DNS query and response messages. Are then sent over UDP or TCP?

>>> UDP

What is the destination port for the DNS query message? What is the source port of DNS response message?

>>> 53; 53

To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

>>> 192.168.254.245; 101.76.223.254; No

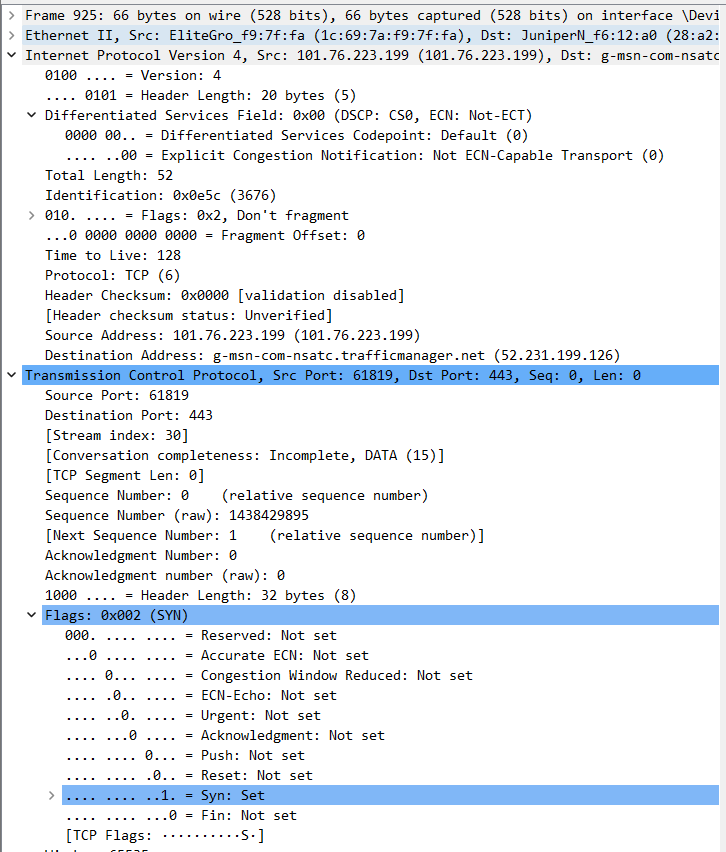
Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

>>> type CNAME; Answer RRs: 0

Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

>>> Answer RRs: 3; Name, Type, Class, TTL, DL, CNAME

Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?



>>> No

This web page contains images. Before retrieving each image, does your host issue new DNS queries?

>>> No

What is the destination port for the DNS query message? What is the source port of DNS response message

>>> 53

To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

>>> 192.168.254.245; Yes

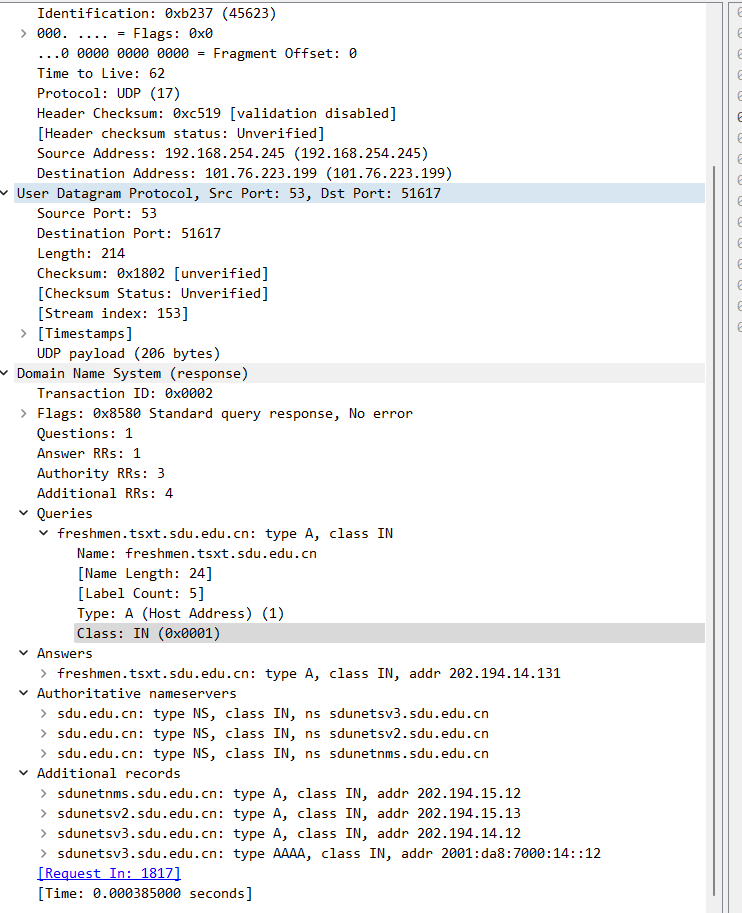
Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

>>> type=A; answer RRs:0

Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

>>> 1;

Provide a screenshot.

>>> 

To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

>>> 192.168.254.245; Yes

Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

>>>type=NS; answer RRs: 0

Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

>>> 1

Provide a screenshot.

>>> 