**Southern University of Science and Technology**

**Computer Networking Lab Report**

**唐润哲 11710418**

* ***Introduction：***

***#Lab5.1***

* + make an DNS query which will invoke the EDNS0
    - Screenshot on this command and its output
  + capture the packages using Wireshark
    - what is the content of this query message
      * Find the name, type and class of this query
      * How can you tell this DNS query is based on EDNS0
      * From this query massage , can it handle DNSSEC security RRs or not
    - what is the content of this response message
      * Is there any answers, what’s the ttl of each answer
      * Is there any authority RRs, what’s the type of each RR
      * Is there any special additional RRs with OPT type, what does its ‘Do bit’ say: Does it accept DNSSEC security RRs or not

***#Lab5.2***

* Make the query by using query method of “dns resolver”(a python package)
  + To query the type A value of www.sina.com.cn based on TCP and UDP stream respectively
* capture the related TCP stream and UDP stream using Wireshark
  + Screenshot on this two commands .
  + what’s the default transport lay protocol while invoke DNS query
* Screenshot on the TCP stream of query by TCP.
* how many TCP packets are captured in this stream, Which port is used?
* Screenshot on the UDP stream of query by UDP.
* how many UDP packets are captured in this stream, Which port is used?
* Is there any difference on DNS query and response message while using TCP and UDP respectively
* ***Procedure***

***#Lab5.1***

1. Open terminal to dig @ns2.sustech.edu.cn www.google.com
2. Use wireshark to capture packages

***#Lab5.2***

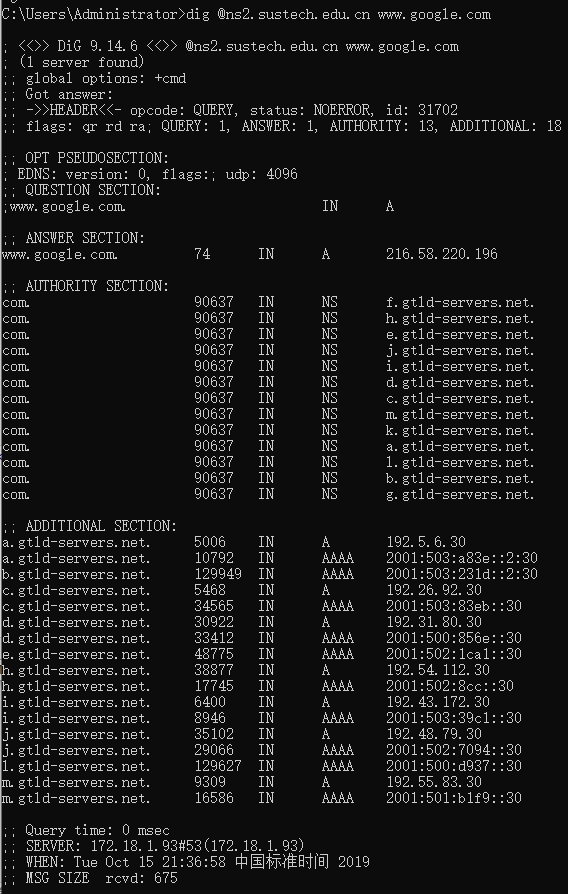
1. Make the query by using query method of “dns resolver”

②capture the related TCP stream and UDP stream using Wireshark

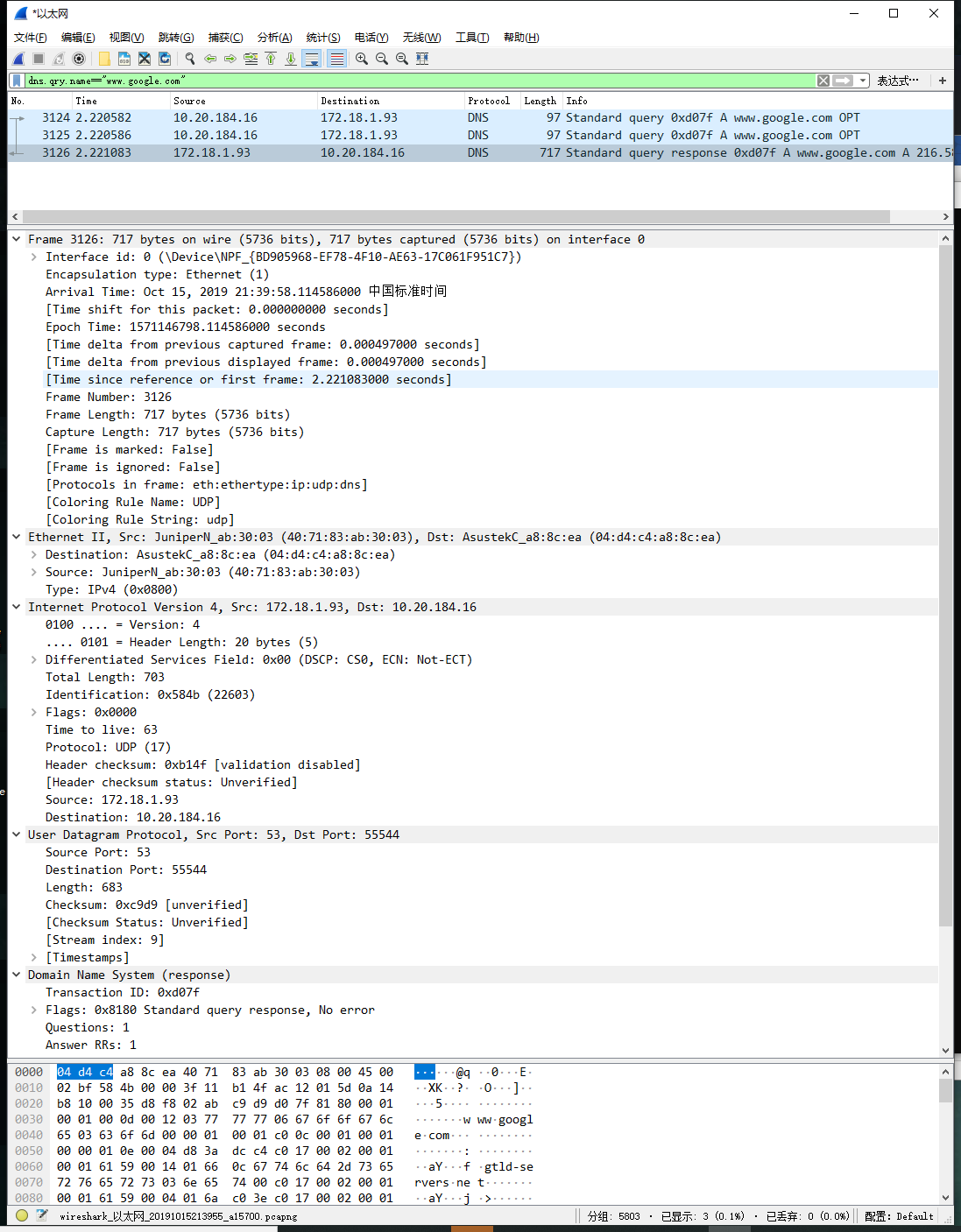
* ***Result：***

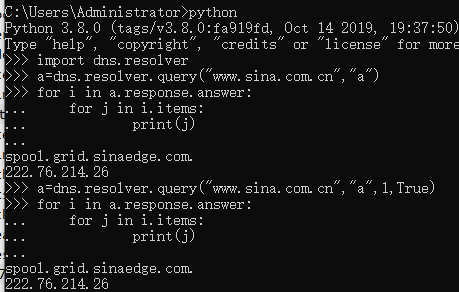
***#Lab5.1***

* + make an DNS query which will invoke the EDNS0



* + capture the packages using Wireshark



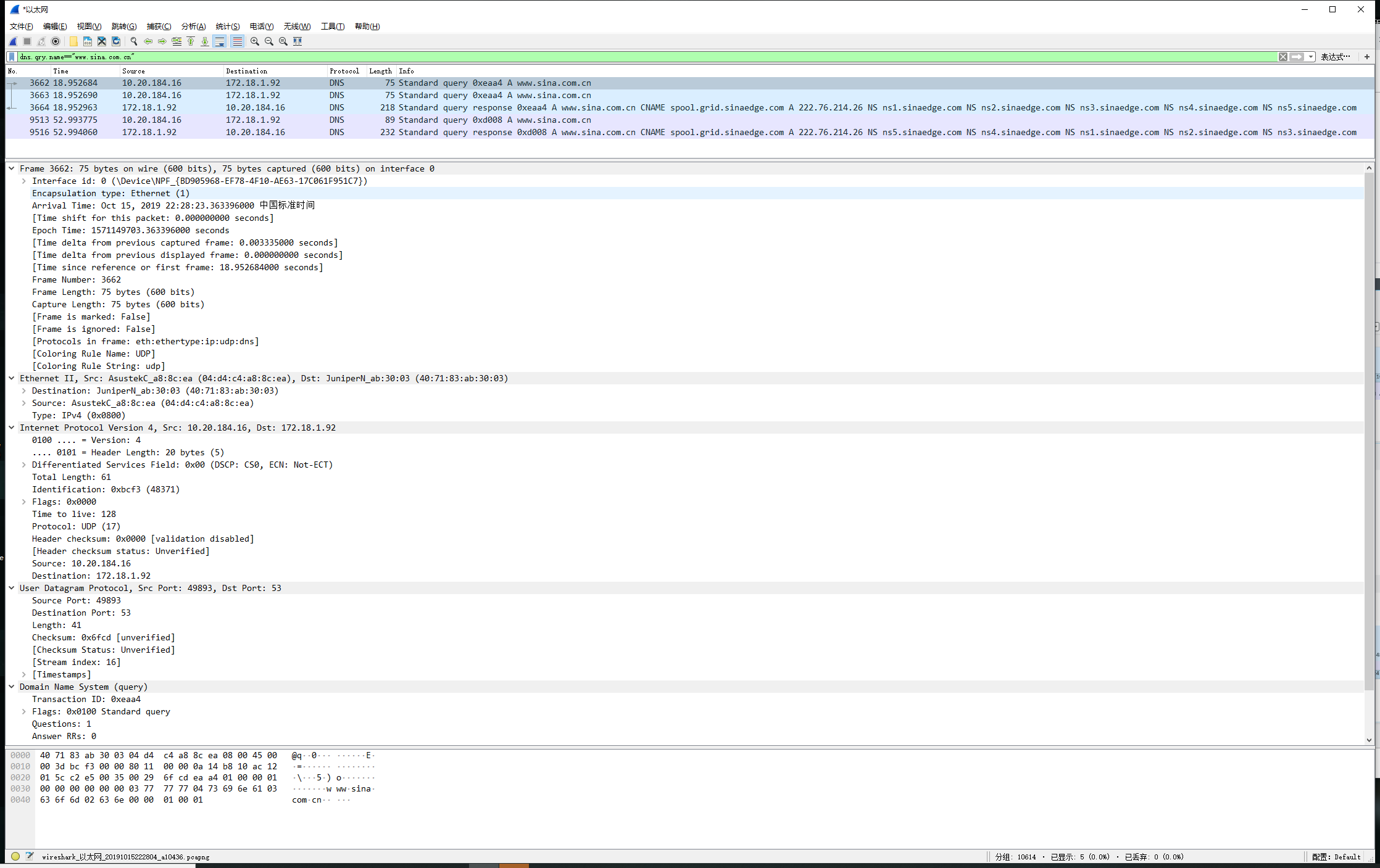
***#Lab5.2***

* + To query the type A value

of www.sina.com.cn

based on TCP and UDP

stream respectively

* + capture the related TCP stream and UDP stream using Wireshark
* ***Conclusion and Experience：***

***#Lab5.1***

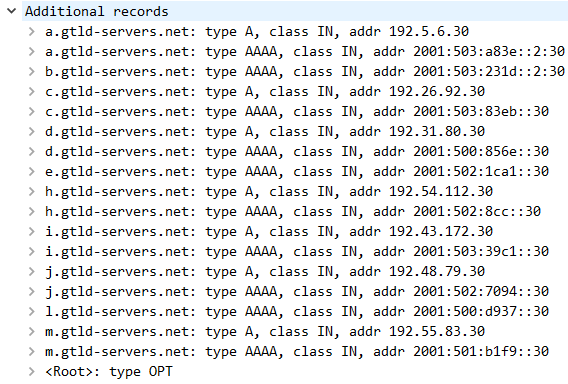
* + *make an DNS query which will invoke the EDNS0*

*Answer: The screenshot is shown above.*

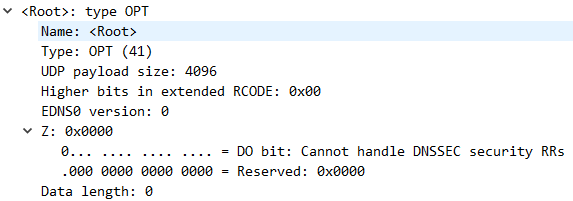
* + *capture the packages using Wireshark*
    - *what is the content of this query message*
      * *Find the name, type and class of this query*

*Answer:*

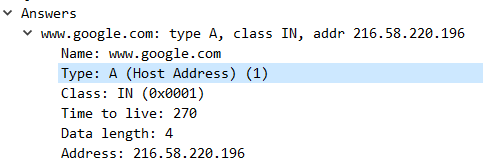
* + - * 1. *Name: www.google.com*
        2. *Type: A(Type: AAAA for IPv6 Address)*
        3. *Class: In*
      * How can you tell this DNS query is based on EDNS0

*Answer: <Root>:type OPT can be found in the Additional records*

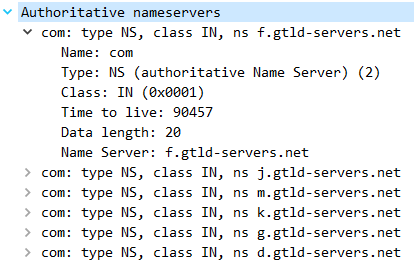
* + - * From this query massage , can it handle DNSSEC security RRs or not

*Answer: It can not handle DNSSEC security RRs*

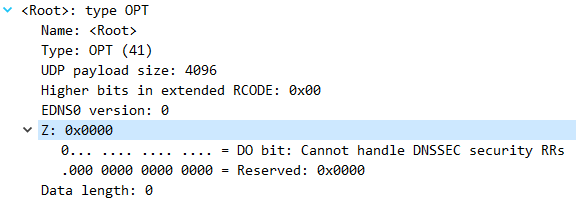
* + - what is the content of this response message
      * Is there any answers, what’s the ttl of each answer

*Answer: The ttl of each answer is 270*

* + - * Is there any authority RRs, what’s the type of each RR

*Answer: There are several authority RRs, and their types are NS(authoritative Name Server)*

* + - * Is there any special additional RRs with OPT type, what does its ‘Do bit’ say: Does it accept DNSSEC security RRs or not

*Answer: There is one special additional RRs with OPT type ,and it does not accept DNSSEC security RRs*

***#Lab5.2***

* Make the query by using query method of “dns resolver”(a python package)
  + To query the type A value of www.sina.com.cn based on TCP and UDP stream respectively

*Answer: The screenshot above is the result.*

*UDP stream: dns.resolver.query("www.sina.com.cn","a")*

*TCP stream:dns.resolver.query("www. sina.com.cn ","a",1,"True")*

* capture the related TCP stream and UDP stream using Wireshark
  + Screenshot on this two commands .

*Answer: The screenshot above is the result.*

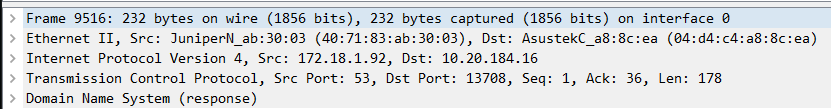
what’s the default transport lay protocol while invoke DNS query

*Answer: The default transport lay protocol is UDP.*

* Screenshot on the TCP stream of query by TCP.

*Answer: The screenshots are shown below(red lines)*





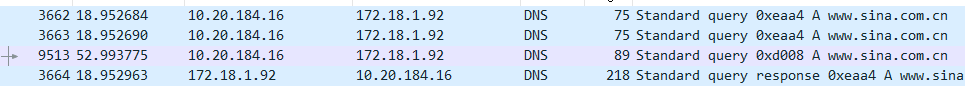
how many TCP packets are captured in this stream, Which port is used?

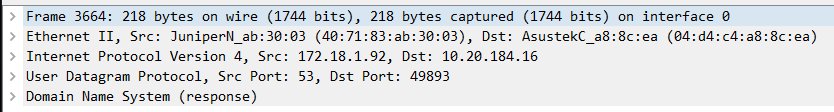
*Answer:* *2 TCP packets are captured.*

*The port used by DNS Server is 53.*

* Screenshot on the UDP stream of query by UDP.

*Answer: The screenshots are shown below(blue lines)*





how many UDP packets are captured in this stream, Which port is used?

*Answer: 2 UCP packets are captured.*

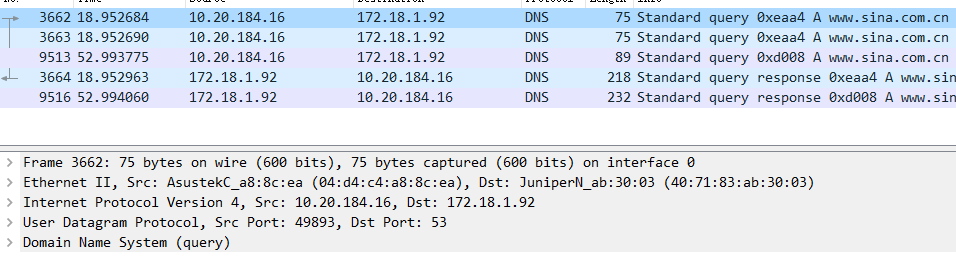
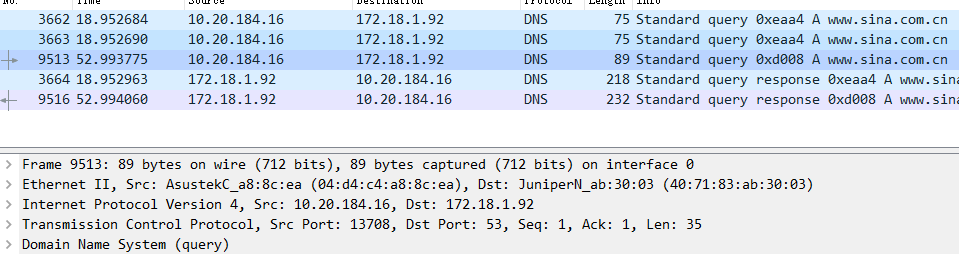
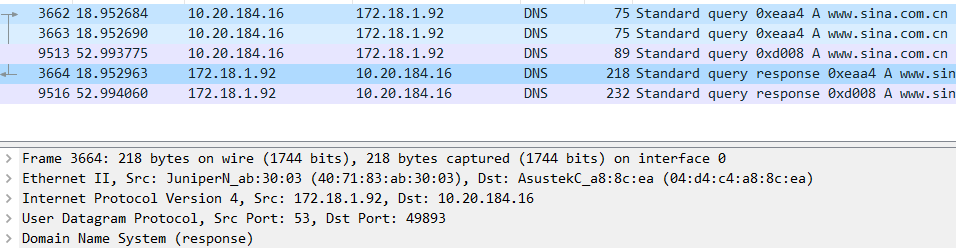
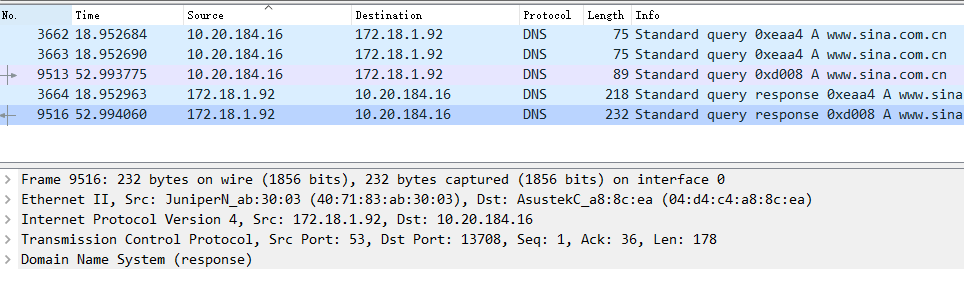
*The port used by DNS Server is 53.*

*(Attention: As shown in the screenshot below, an error happened so a dns query retransmission is acted,so in the screenshot above,there are 3 UDP packets.*



* Is there any difference on DNS query and response message while using TCP and UDP respectively

*Answer: From screenshots below, we can know that when we use TCP, we will get packets' length ,which can not be transferred by UDP.*

* + - Query:
      * UDP:
      * TCP:
    - Response:
      * UDP:
      * TCP: