電腦網路作業：Wireshark Lab: DNS

S1154041 邱立宇

1.Run nslookup to obtain the IP address of the web server for the Indian Institute of Technology in Bombay, India: www.iitb.ac.in. What is the IP address of www.iitb.ac.in?

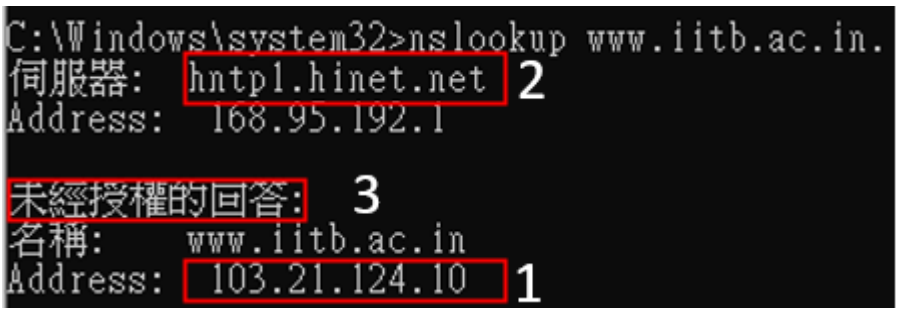
Ans: 103.21.124.10

2. What is the IP address of the DNS server that provided the answer to your nslookup command in question 1 above?

Ans:hntp1.hinet.net

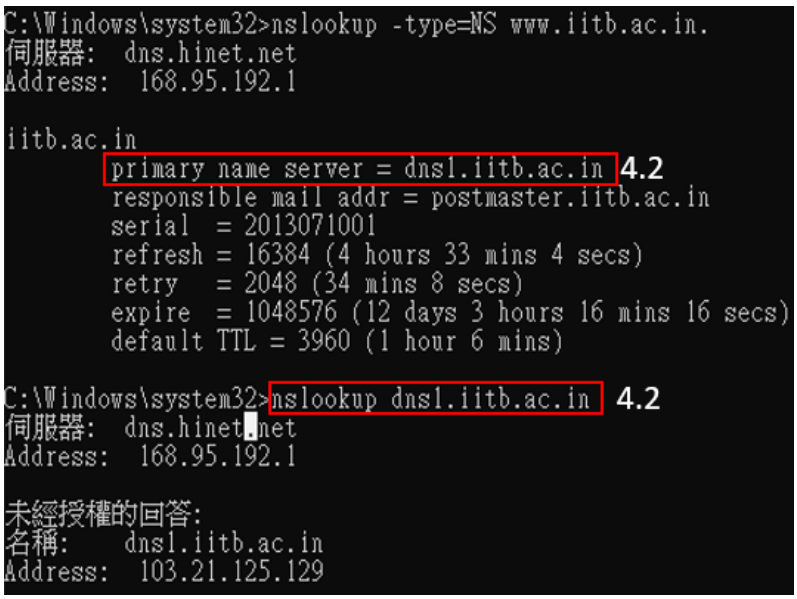
3. Did the answer to your nslookup command in question 1 above come from an authoritative or non-authoritative server?

Ans: non-authoritative



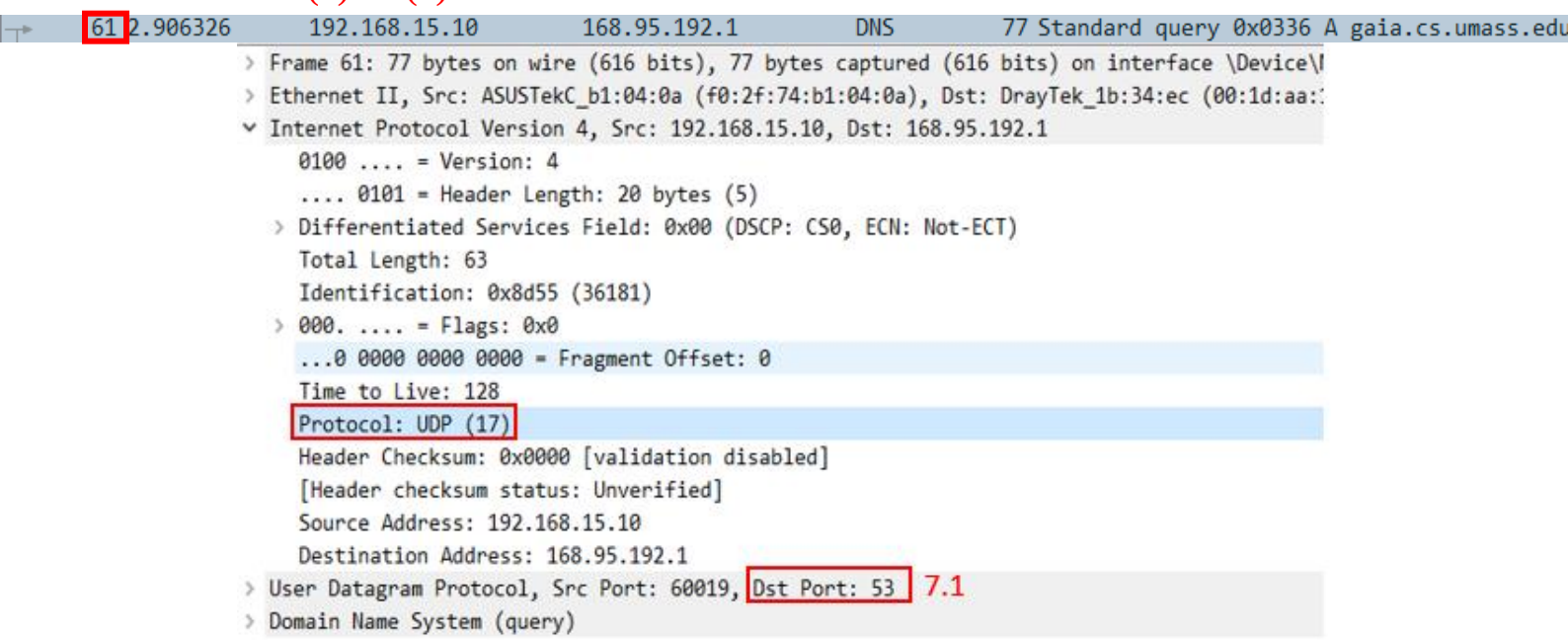
4. Use the nslookup command to determine the name of the authoritative name server for the iit.ac.in domain. What is that name? (If there are more than one authoritative servers, what is the name of the first authoritative server returned by nslookup)? If you had to find the IP address of that authoritative name server, how would you do so?

Ans: (1) dns1.iitb.ac.in (2) nslookup dns1.iitb.ac.in



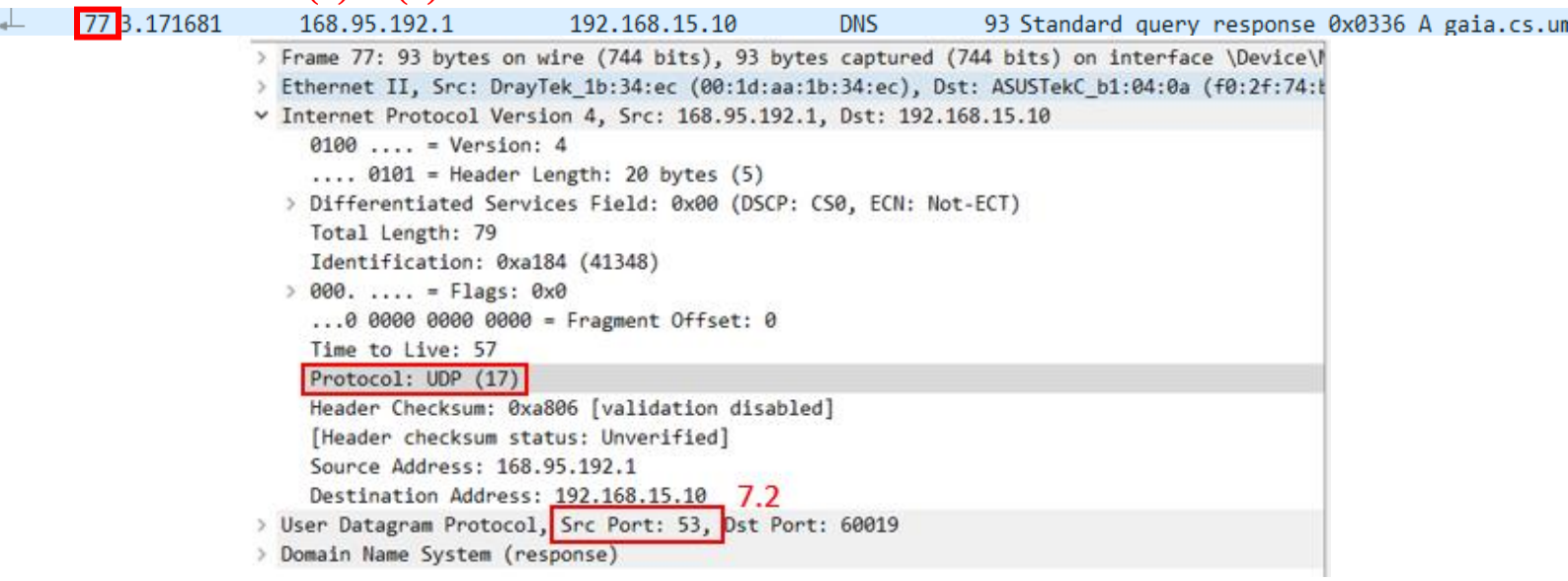
5. Locate the first DNS query message resolving the name gaia.cs.umass.edu. What is the packet number in the trace for the DNS query message? Is this query message sent over UDP or TCP?

Ans:(1) 61 (2) UDP



6. Now locate the corresponding DNS response to the initial DNS query. What is the packet number in the trace for the DNS response message? Is this response message received via UDP or TCP?

Ans:(1)77 (2) UDP



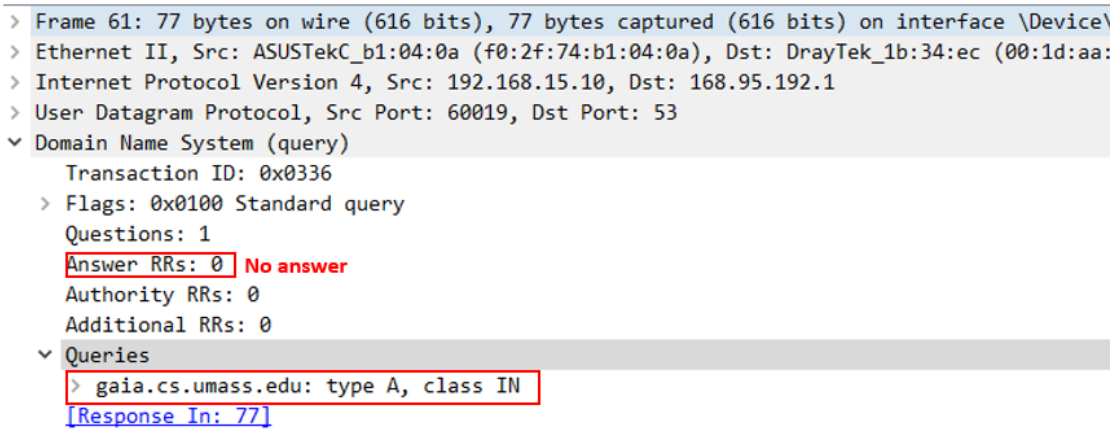
7. What is the destination port for the DNS query message? What is the source port of the DNS response message?

Ans: Both 53

8. To what IP address is the DNS query message sent? Ans: 168.95.192.1

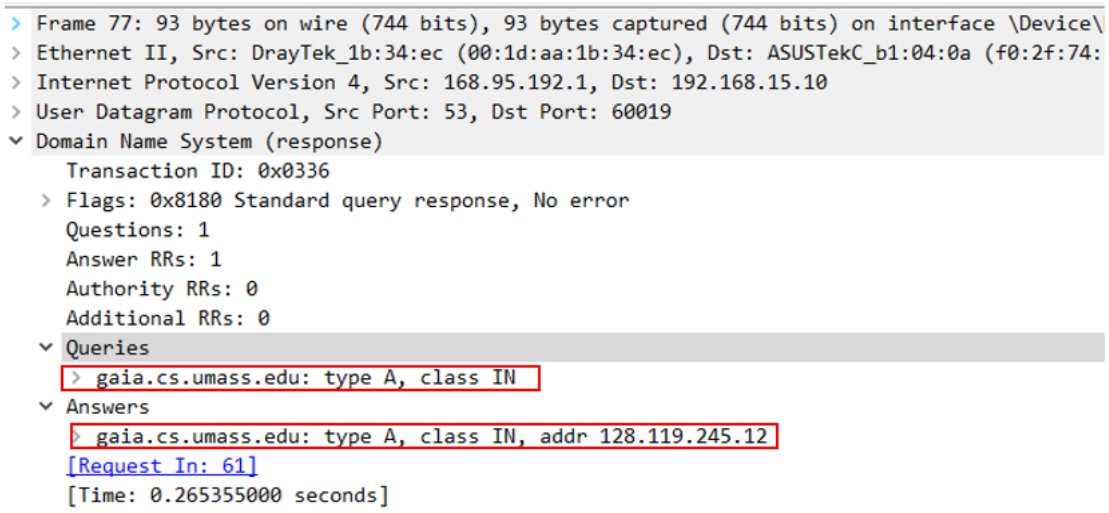
9. Examine the DNS query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain?

Ans:(1) 1 (2) 0

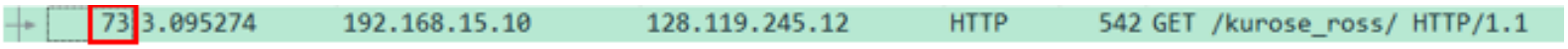


10. Examine the DNS response message to the initial query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain?

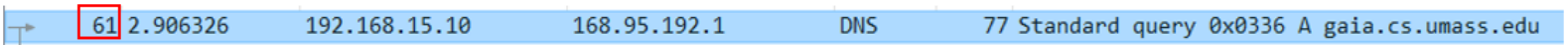
Ans:(1) 1 (2) 1



11. The web page for the base file http://gaia.cs.umass.edu/kurose_ross/ references the image object http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg , which, like the base webpage, is on gaia.cs.umass.edu. What is the packet number in the trace for the initial HTTP GET request for the base file http://gaia.cs.umass.edu/kurose_ross/?



What is the packet number in the trace of the DNS query made to resolve gaia.cs.umass.edu so that this initial HTTP request can be sent to the gaia.cs.umass.edu IP address?



What is the packet number in the trace of the received DNS response?

What is the packet number in the trace for the HTTP GET request for the image object http://gaia.cs.umass.edu/kurose_ross/ header_graphic_book _8E2.jpg?

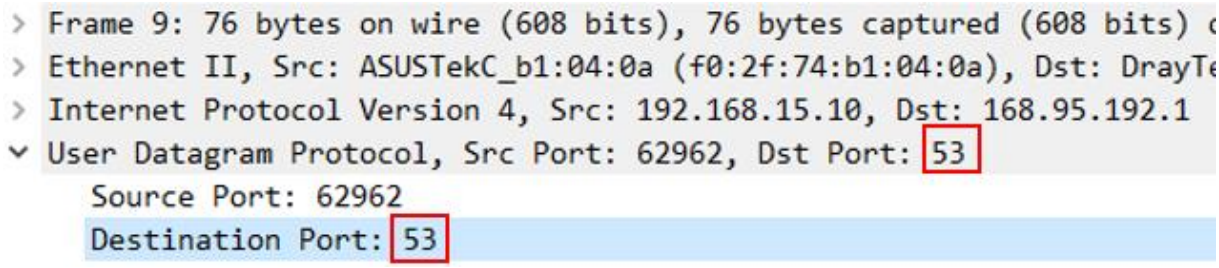
What is the packet number in the DNS query made to resolve gaia.cs.umass.edu so that this second HTTP request can be sent to the gaia.cs.umass.edu IP address?

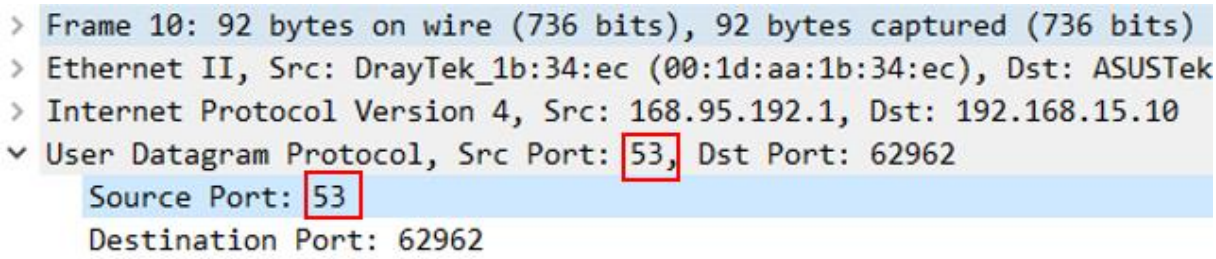
Discuss how DNS caching affects the answer to this last question.

Ans: (1)73 (2)61 (3)77 (4)279 (5)61 (6)Since the domain has been resolved, the following requests to this domain don't need to solve again.

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

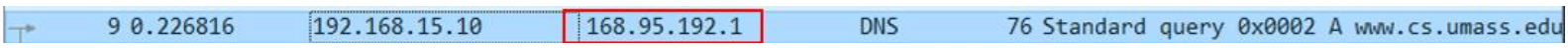
Ans: Both 53

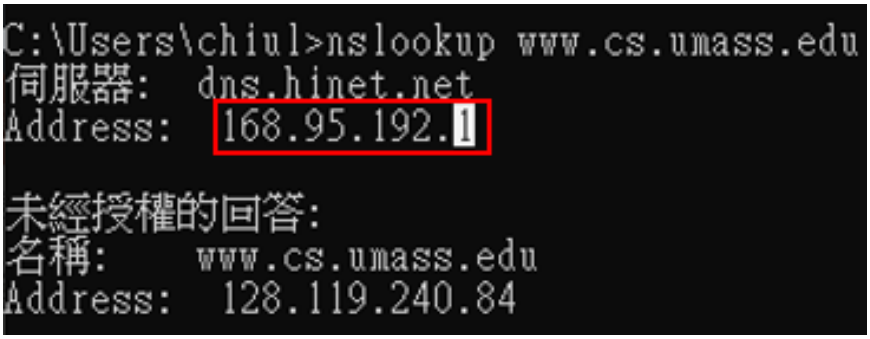




13. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

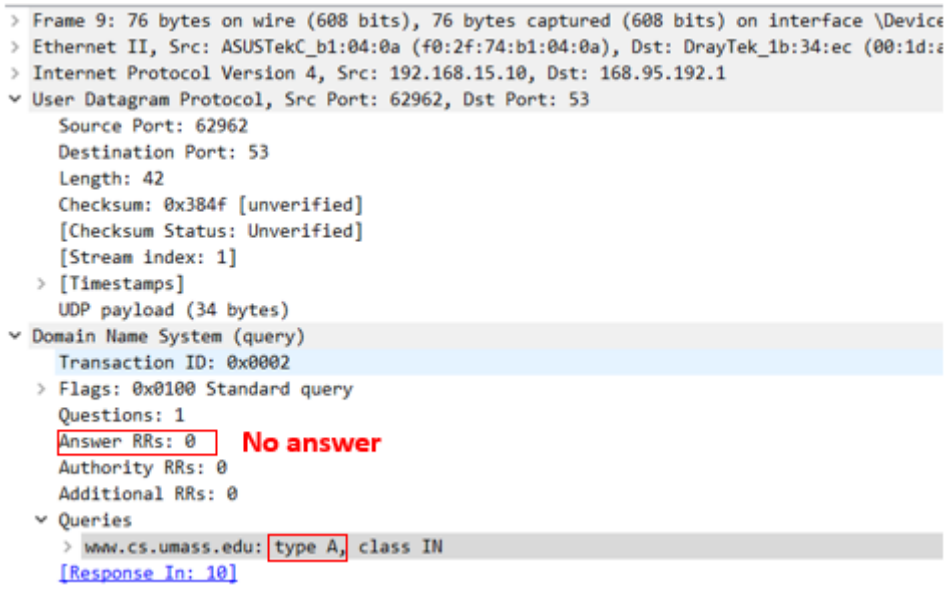
Ans: (1)168.95.192.1(2)YES





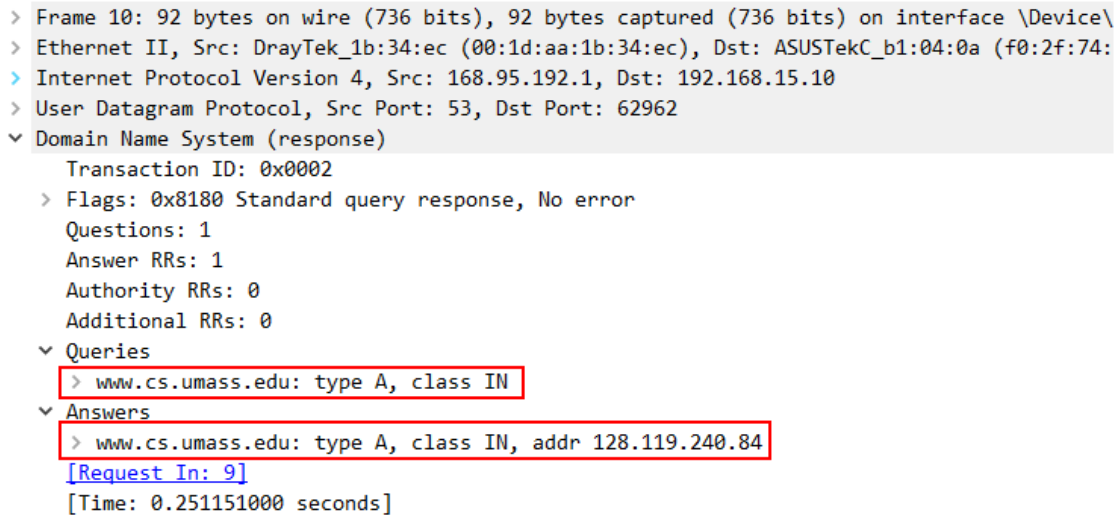
14. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

Ans:(1)A (2) NO



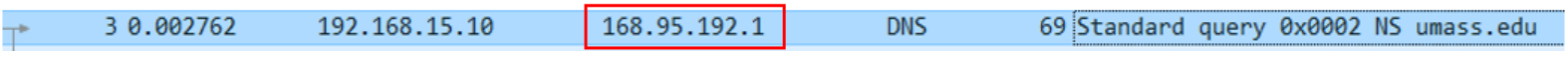
15. Examine the DNS response message to the query message. How many "questions" does this DNS response message contain? How many "answers"?

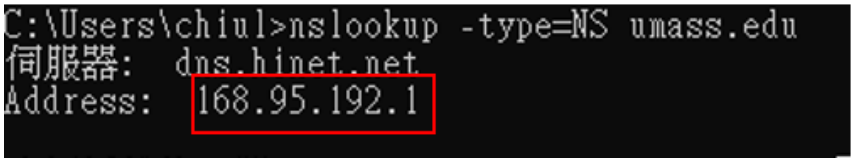
Ans:(1) 1 (2) 1



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

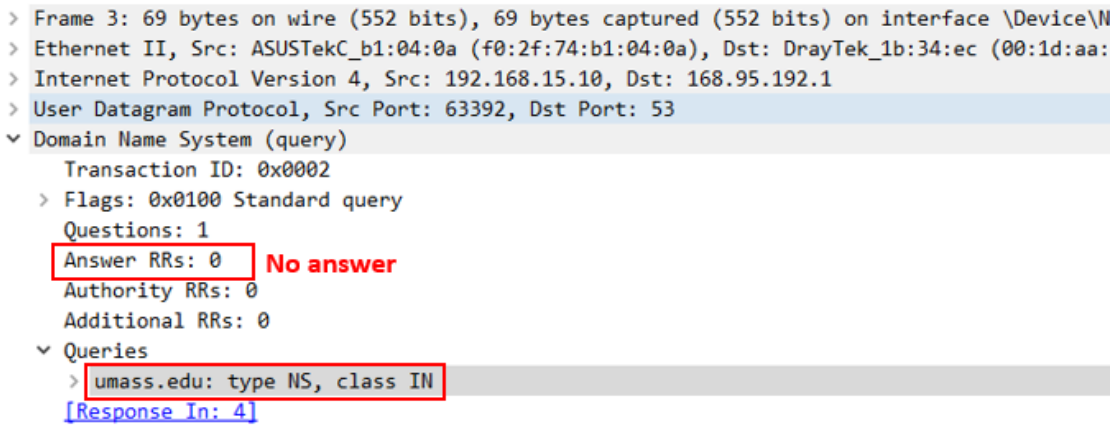
Ans: (1)168.95.192.1(2)YES





17. Examine the DNS query message. How many questions does the query have? Does the query message contain any “answers”?

Ans: (1) 1 (2) NO



18. Examine the DNS response message. How many answers does the response have? What information is contained in the answers? How many additional resource

Ans: (1) 3 (2) umass.edu domain’s nameserver (3) 0