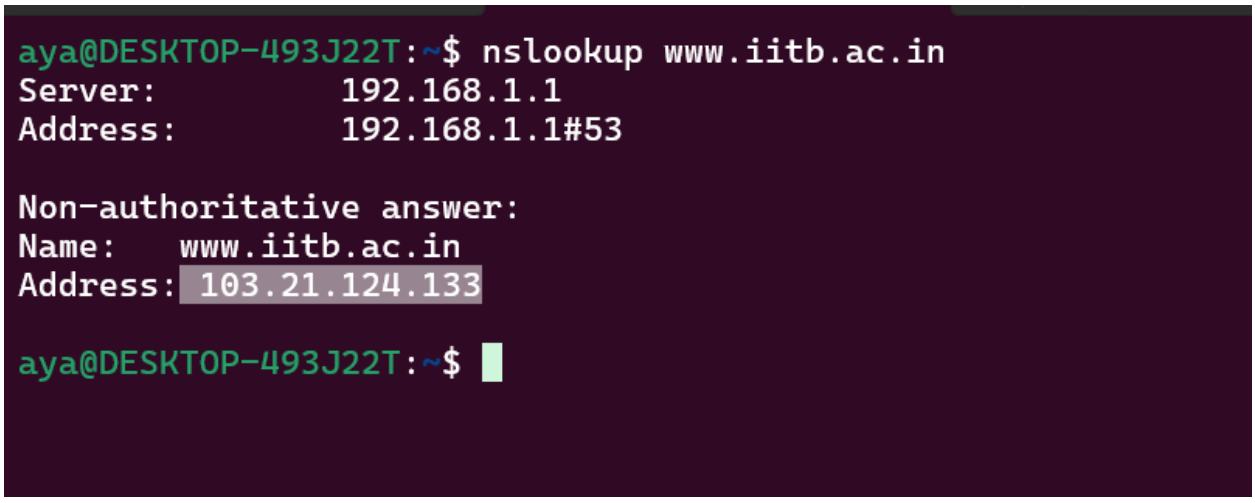
Name: Aya Salah Eldine

Id: 7361

Lab4

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



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

```
aya@DESKTOP-493J22T:~$ nslookup www.iitb.ac.in
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   www.iitb.ac.in
Address: 103.21.124.133

aya@DESKTOP-493J22T:~$
```

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

```
aya@DESKTOP-493J22T:~$ nslookup www.iitb.ac.in
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   www.iitb.ac.in
Address: 103.21.124.133

aya@DESKTOP-493J22T:~$
```

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?

```
aya@DESKTOP-493J22T:~$ nslookup -type=NS iitb.ac.in
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
iitb.ac.in      nameserver = dns3.iitb.ac.in.
iitb.ac.in      nameserver = dns2.iitb.ac.in.
iitb.ac.in      nameserver = dns1.iitb.ac.in.

Authoritative answers can be found from:

aya@DESKTOP-493J22T:~$
```

5-Repeat the previous 4 steps using Python programming language and with the aid of the following packages:

- **socket — Low-level networking interface — Python 3.12.3 documentation**
- **The dns.resolver.Resolver and dns.resolver.Answer Classes — dnspython 2.6.1 documentation from (dnspython · PyPI**

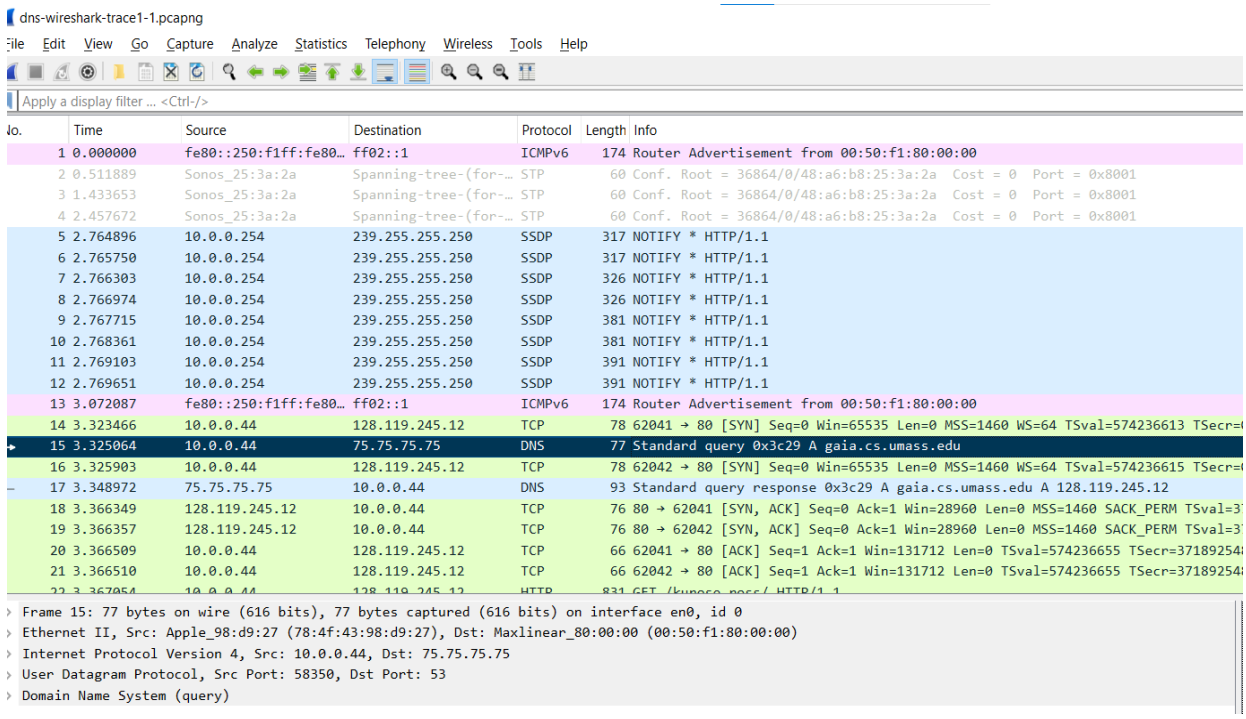
Welcome import socket Untitled-1 1

```python
import socket
import dns.resolver

# 1. Get the IP address of www.iitb.ac.in
def get_ip_address(hostname):
    try:
        ip_address = socket.gethostbyname(hostname)
        return ip_address
    except socket.error as e:
        print(f"Error: {e}")
        return None

iitb_ip = get_ip_address('www.iitb.ac.in')
print(f"1. IP address of www.iitb.ac.in: {iitb_ip}")

# 2. Get the IP address of the DNS server that provided the answer
resolver = dns.resolver.Resolver()
try:
    response = resolver.resolve('www.iitb.ac.in')
    dns_server_ip = resolver.nameservers[0]  # Get the first DNS server used by the resolver
    print(f"2. IP address of the DNS server that provided the answer: {dns_server_ip}")
except dns.resolver.NoAnswer:
    print("No DNS server found")
except dns.exception.DNSException as e:
    print(f"DNS Exception: {e}")

# 3. Determine if the answer is authoritative or non-authoritative
try:
    response = resolver.resolve('www.iitb.ac.in', 'A', raise_on_no_answer=False)
    if response.rrset:
        if response.rrset.ttl == 0:
            print("3. The answer is authoritative.")
        else:
            print("3. The answer is non-authoritative.")
    else:
        print("3. No answer found.")
except dns.resolver.NoAnswer:
    print("3. No answer found.")

# 4. Get the authoritative name server for the iit.ac.in domain
domain = "iitb.ac.in"
record_type = "NS"

try:
    response = resolver.resolve(domain, record_type)
    nameservers = [str(ns) for ns in response]
    if nameservers:
        print("4. Authoritative name servers for iitb.ac.in:")
        for nameserver in nameservers:
            print(f"   - {nameserver}")
    else:
        print("4. No authoritative name servers found.")
except dns.resolver.NXDOMAIN:
    print("4. Domain does not exist.")
except dns.resolver.NoAnswer:
    print("4. No authoritative name servers found.")
except dns.resolver.Timeout:
    print("4. DNS query timed out.")
except dns.resolver.ResolverError as e:
```

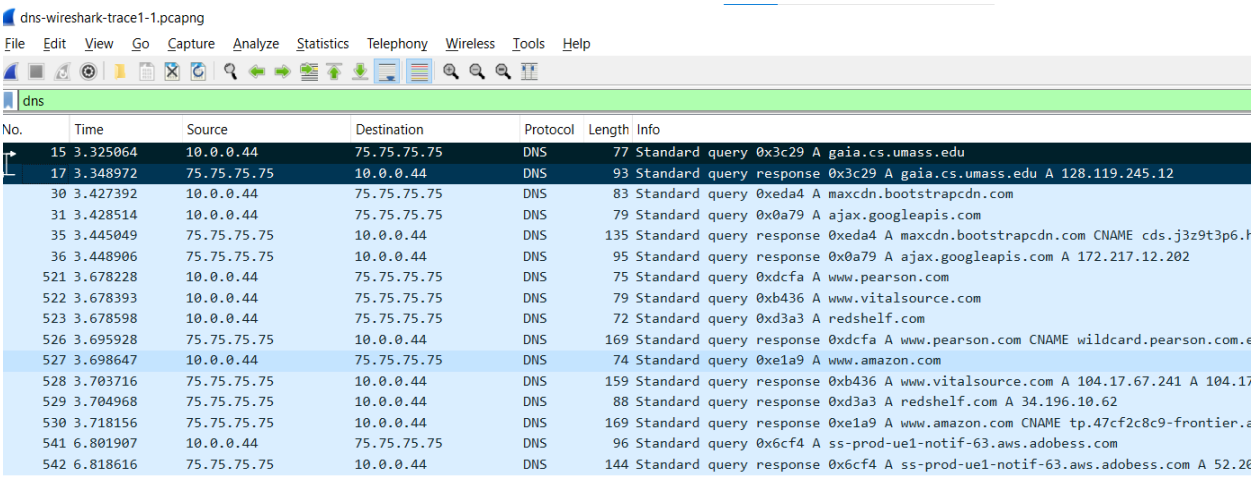
PROBLEMS 1 OUTPUT DEBUG CONSOLE TERMINAL PORTS

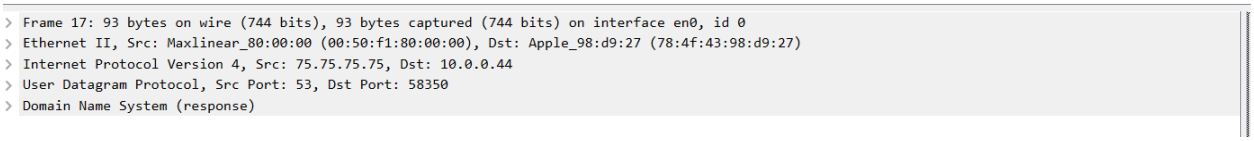
```
PS C:\Users\Dell> python -u "C:\Users\Dell\AppData\Local\Temp\tempCodeRunnerFile.python"
1. IP address of www.iitb.ac.in: 103.21.124.133
2. IP address of the DNS server that provided the answer: 192.168.1.1
3. The answer is non-authoritative.
4. Authoritative name servers for iitb.ac.in:
   - dns3.iitb.ac.in.
   - dns2.iitb.ac.in.
   - dns1.iitb.ac.in.
PS C:\Users\Dell>
```

6-Locate the first DNS query message resolving the name gaia.cs.umass.edu. What is the packet number6 in the trace for the DNS query message? Is this query message sent over UDP or TCP? Udp/15



7-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? 17/udp





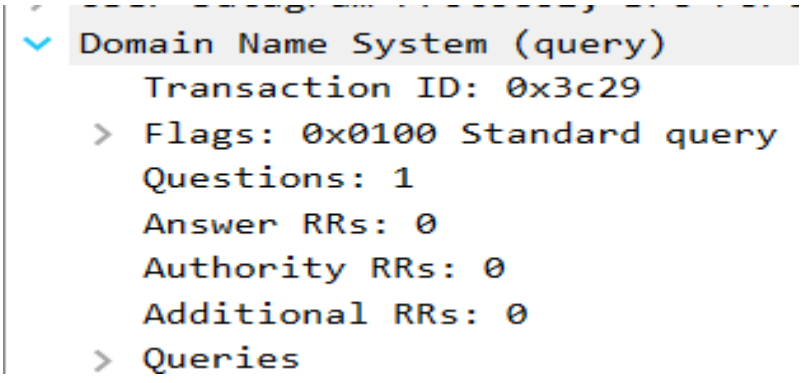
8. What is the destination port for the DNS query message? What is the source port of the DNS response message? 53

9. To what IP address is the DNS query message sent?

75.75.75.75

10.Examine the DNS query message. How many "questions" does this DNS message contain? How many "answers" answers does it contain?

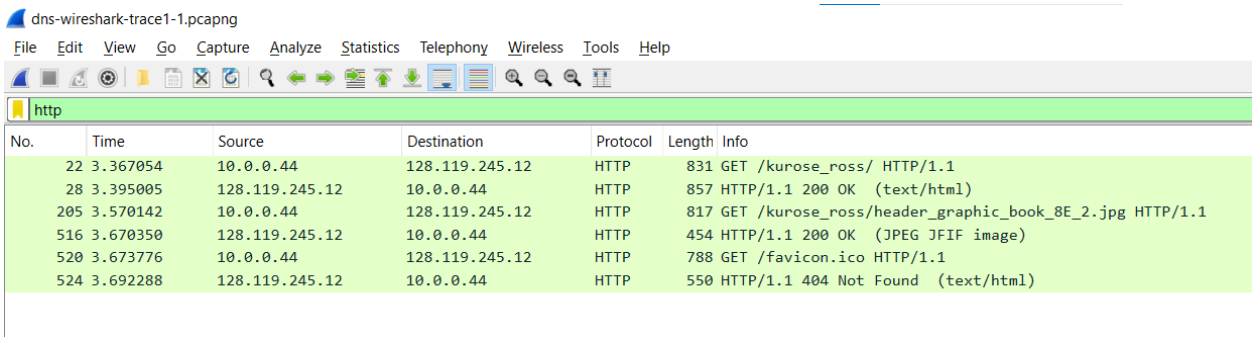
Questions: 1 Answer :0



11.. 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?

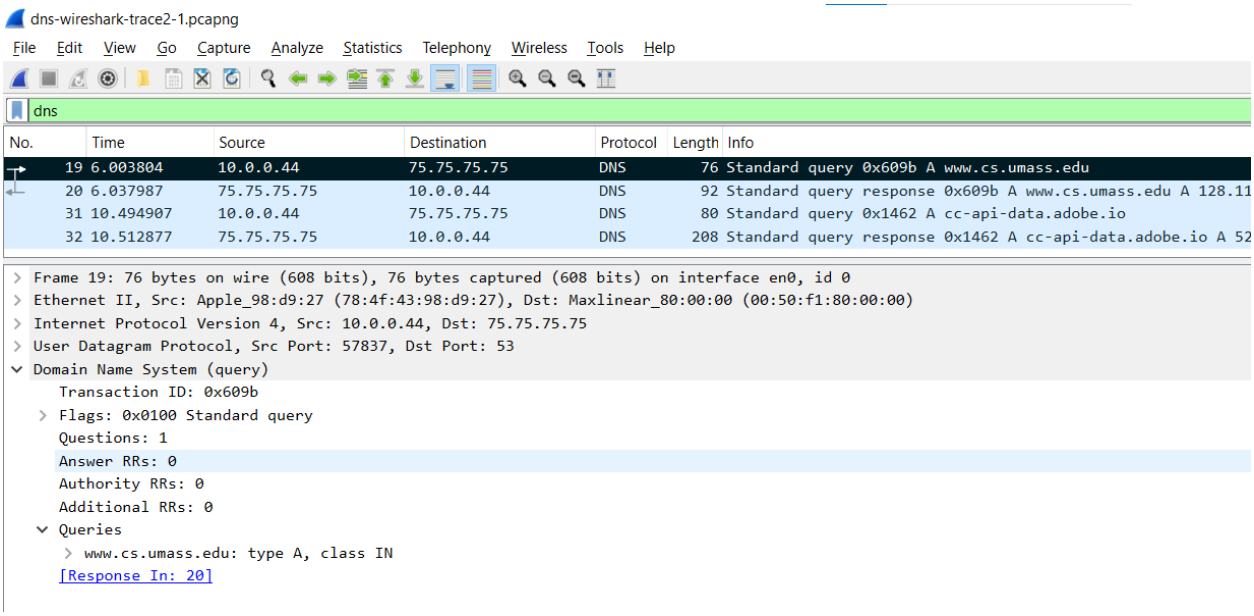
```
Domain Name System (response)
    Transaction ID: 0x3c29
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  Queries
    > gaia.cs.umass.edu: type A, class IN
  Answers
    > gaia.cs.umass.edu: type A, class IN, addr 128.119.245.12
    [Request In: 15]
    [Time: 0.023908000 seconds]
```

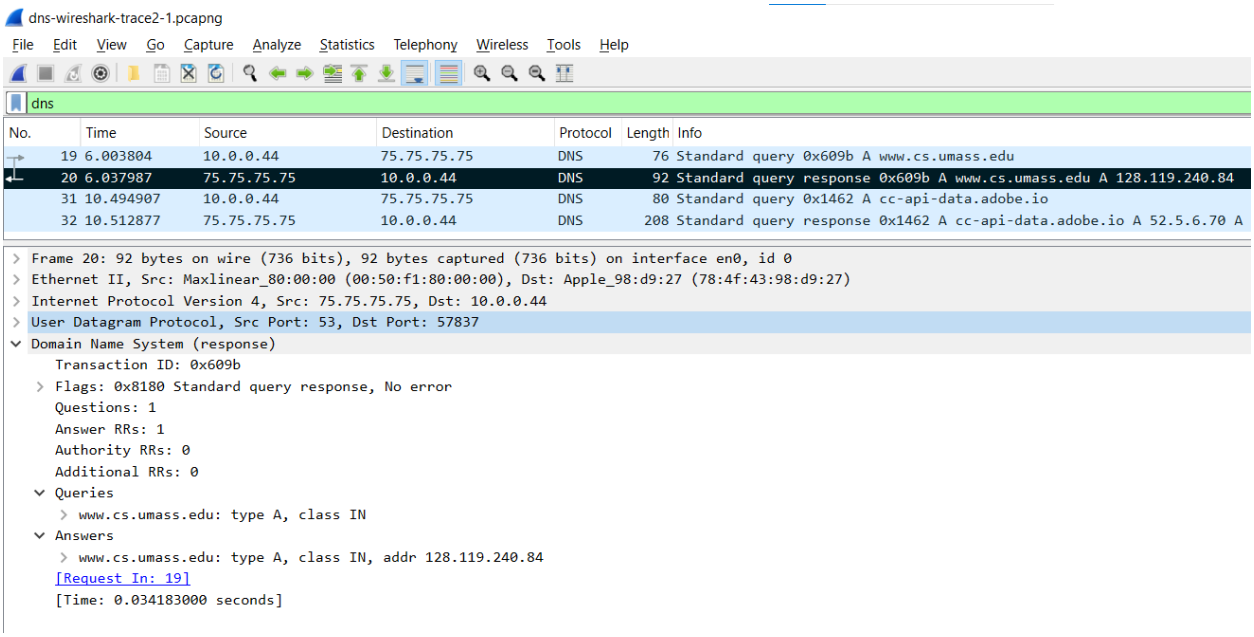
12. 22 – 15 – 17 - 205 – 15 – no because it is cached



No.	Time	Source	Destination	Protocol	Length	Info
22	3.367054	10.0.0.44	128.119.245.12	HTTP	831	GET /kurose_ross/ HTTP/1.1
28	3.395005	128.119.245.12	10.0.0.44	HTTP	857	HTTP/1.1 200 OK (text/html)
205	3.570142	10.0.0.44	128.119.245.12	HTTP	817	GET /kurose_ross/header_graphic_book_8E_2.jpg HTTP/1.1
516	3.670350	128.119.245.12	10.0.0.44	HTTP	454	HTTP/1.1 200 OK (JPEG JFIF image)
520	3.673776	10.0.0.44	128.119.245.12	HTTP	788	GET /favicon.ico HTTP/1.1
524	3.692288	128.119.245.12	10.0.0.44	HTTP	550	HTTP/1.1 404 Not Found (text/html)

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

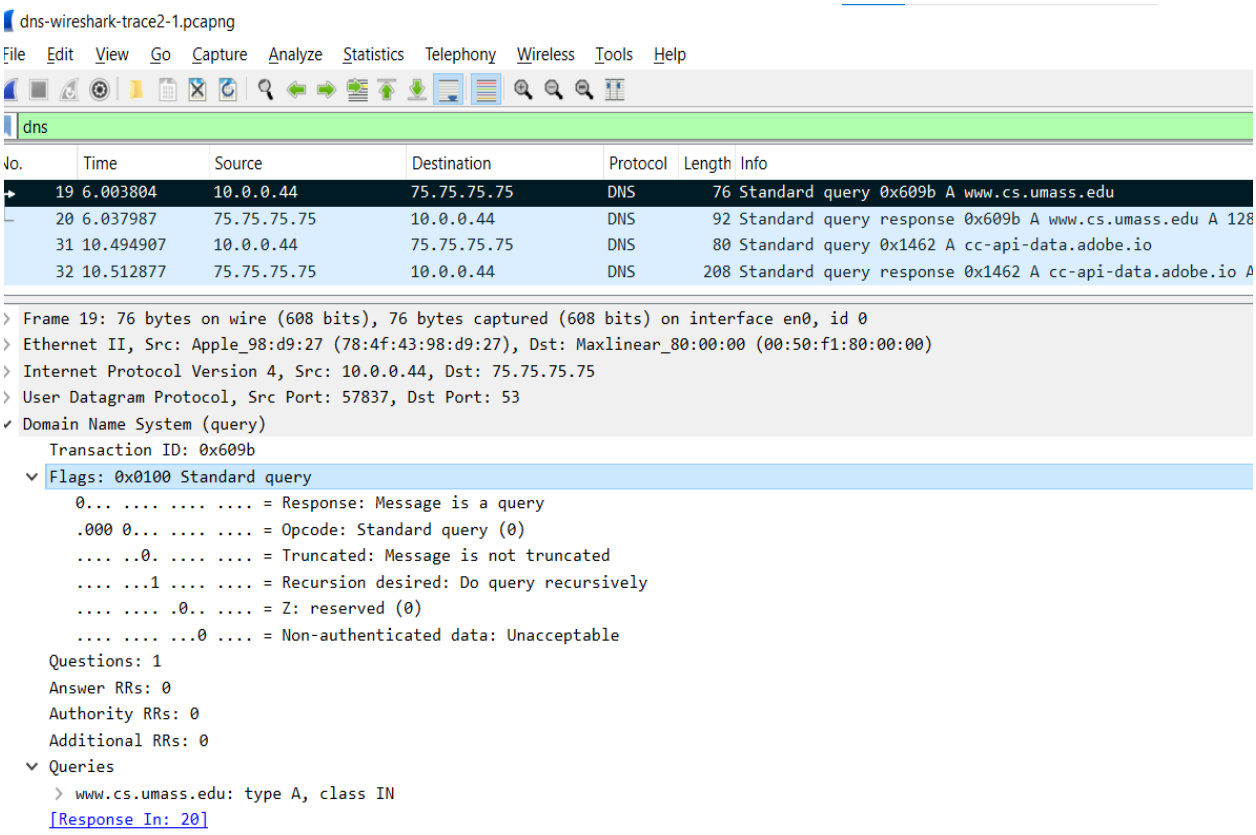




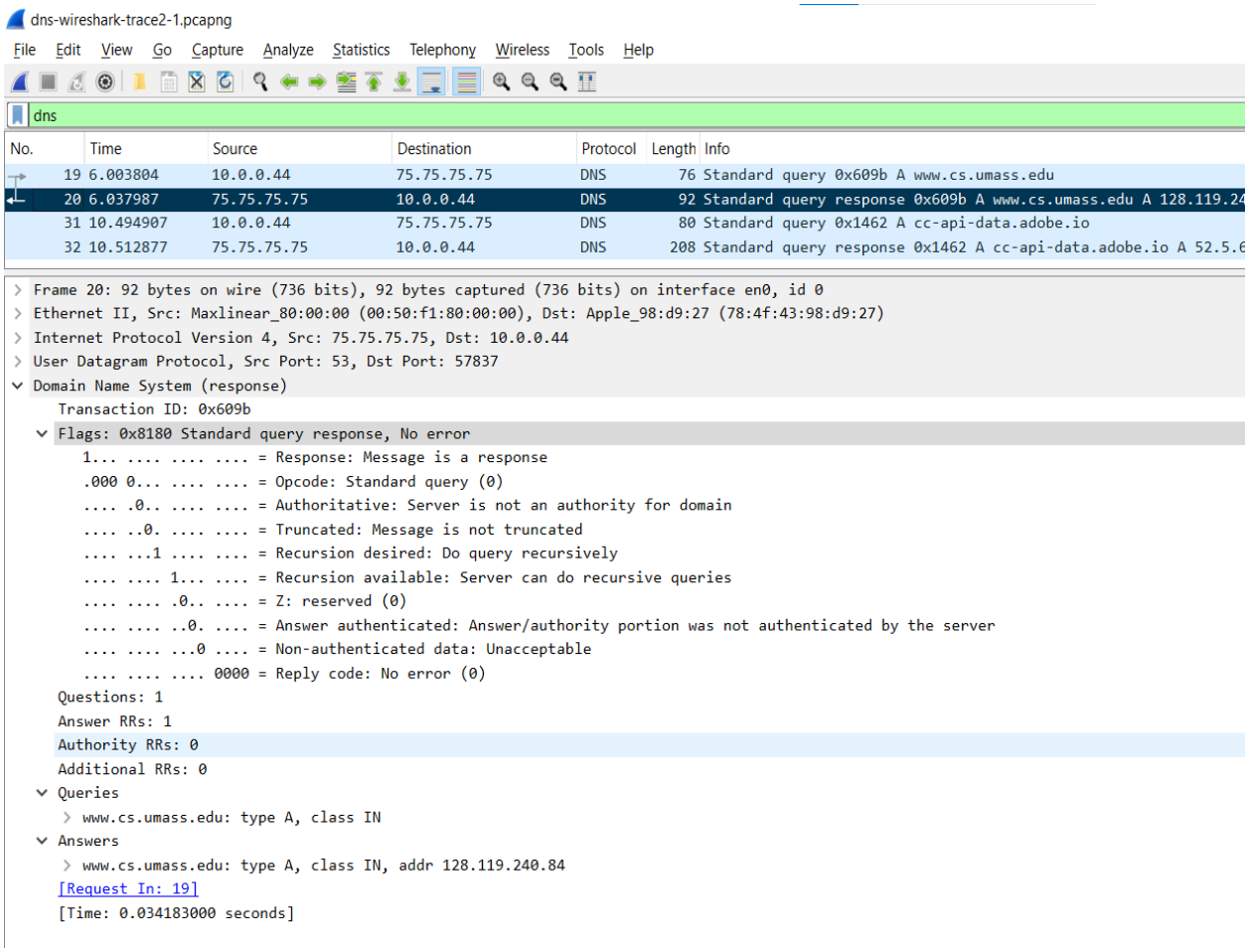
14.To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

75.75.75.75 – yes

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



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



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

75.75.75.75 – yes

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

Questions: 1 Answer :0

19. Examine the DNS response message (in particular the DNS response message that has type “NS”). How many answers does the response have? What information is contained in the answers? How many additional resource records are returned? What additional information is included in these additional resource records (if additional information is returned)?