HỌ TÊN : NGUYỄN XUÂN TRỰC

MSSV : 1513804

LỚP : L07

==========o0o==========

Question 01. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

ANSWER

```
Microsoft Windows [Version 10.0.19042.630]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\TRUC BK>nslookup www.thanhnien.vn
Server:  UnKnown
Address:  192.168.43.2

Non-authoritative answer:
Name:    www.thanhnien.vn
Addresses:  2606:4700:3031::ac43:8a08
          2606:4700:3032::6818:7818
          2606:4700:3034::6818:7918
          104.24.121.24
          172.67.138.8
          104.24.120.24
```

Question 02. Run nslookup to determine the authoritative DNS servers for a university in Europe.

ANSWER

```
C:\Users\TRUC BK>nslooku[ wwww.cambridge.org
'nslooku[' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\TRUC BK>nslookkup www.cambridge.org
'nslookkup' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\TRUC BK>nslookup www.cambridge.org
Server:  UnKnown
Address:  192.168.43.2

Non-authoritative answer:
Name:    www.cambridge.org.cdn.cloudflare.net
Addresses:  104.16.55.52
          104.16.56.52
Aliases:  www.cambridge.org
```

```
C:\Users\TRUC BK>nslookup -type=NS www.cambridge.org
Server:  UnKnown
Address:  192.168.43.2

Non-authoritative answer:
www.cambridge.org       canonical name = www.cambridge.org.cdn.cloudflare.net

cloudflare.net
        primary name server = ns1.cloudflare.net
        responsible mail addr = dns.cloudflare.com
        serial  = 1606975971
        refresh = 10000 (2 hours 46 mins 40 secs)
        retry   = 2400 (40 mins)
        expire  = 604800 (7 days)
        default TTL = 3600 (1 hour)
```

Authoritative DNS servers for a university is: www.cambridge.org.cdn.cloudflare.net

Question 03. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

ANSWER

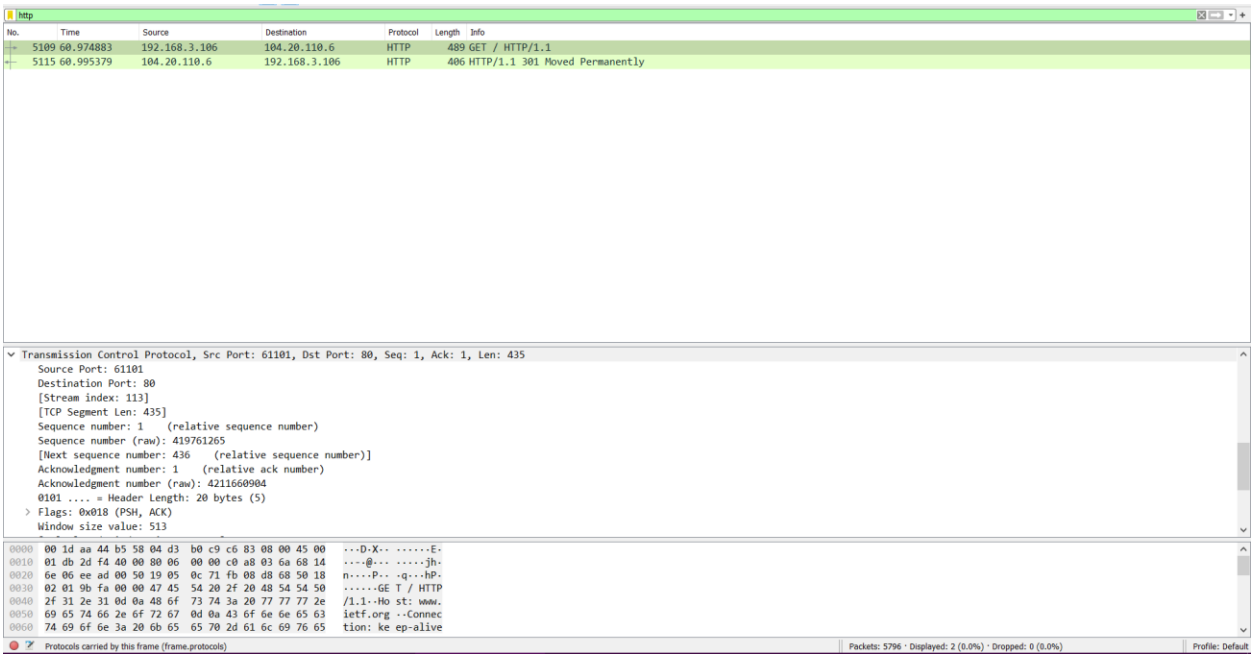
Mail servers is: dns.cloudflare.com

And its IP: 104.16.132.229

104.16.133.229

Question 04. Locate the DNS query and response messages. Are then sent over UDP or TCP?

ANSWER



Được gửi bằng TCP

Question 05. What is the destination port for the DNS query message? What is the source port of DNS response message?

ANSWER

Destination is: 80

Source is : 61101

Question 06. 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?

ANSWER

104.20.110.06

The same

Question 07. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

ANSWER

Type is: Type: IPv4 (0x0800)

No answer.

Question 08. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

ANSWER

1 answer. HTTP/1.1 301 Moved Permanently\r\n…… [HTTP response 1/1]

Question 09. 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?

ANSWER

Yes

Question 10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

ANSWER

No

Question 11. What is the destination port for the DNS query message? What is the source port of DNS response message?

ANSWER

Source port is: 62990

Destination is: 53

Question 12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

ANSWER

192.168.1.1

YES

Question 13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

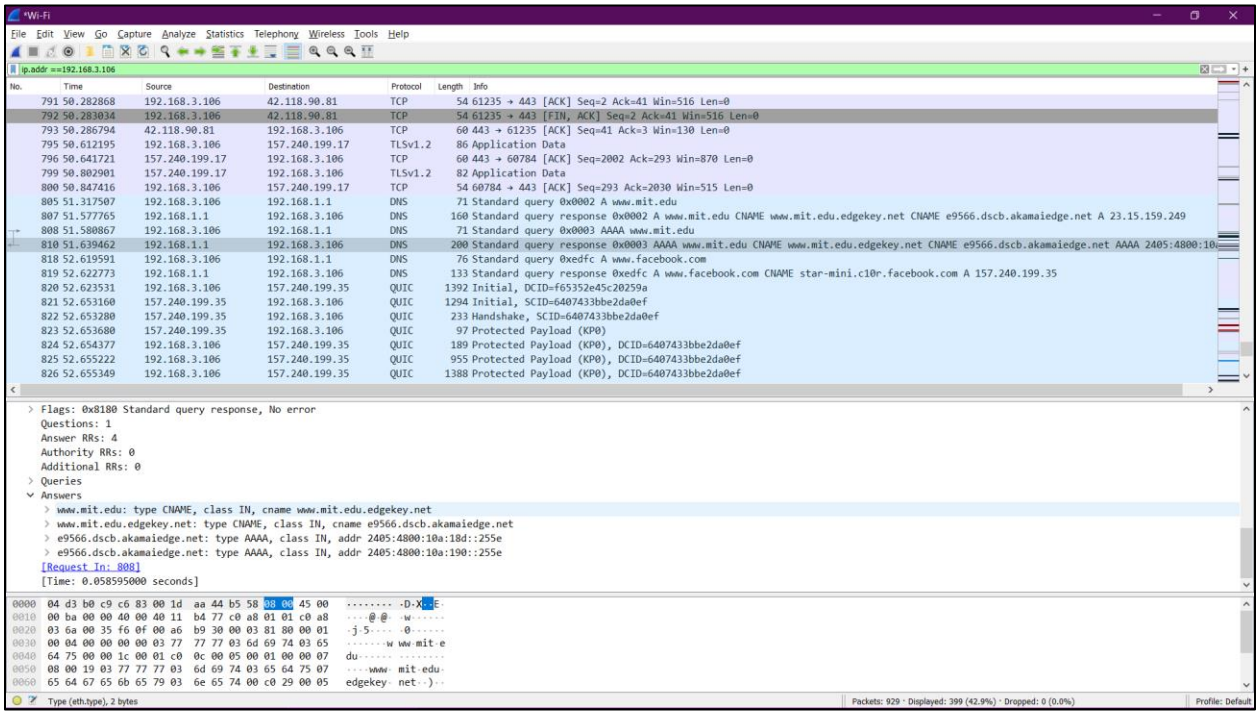
ANSWER

Type is: Type: IPv4 (0x0800).

No answer

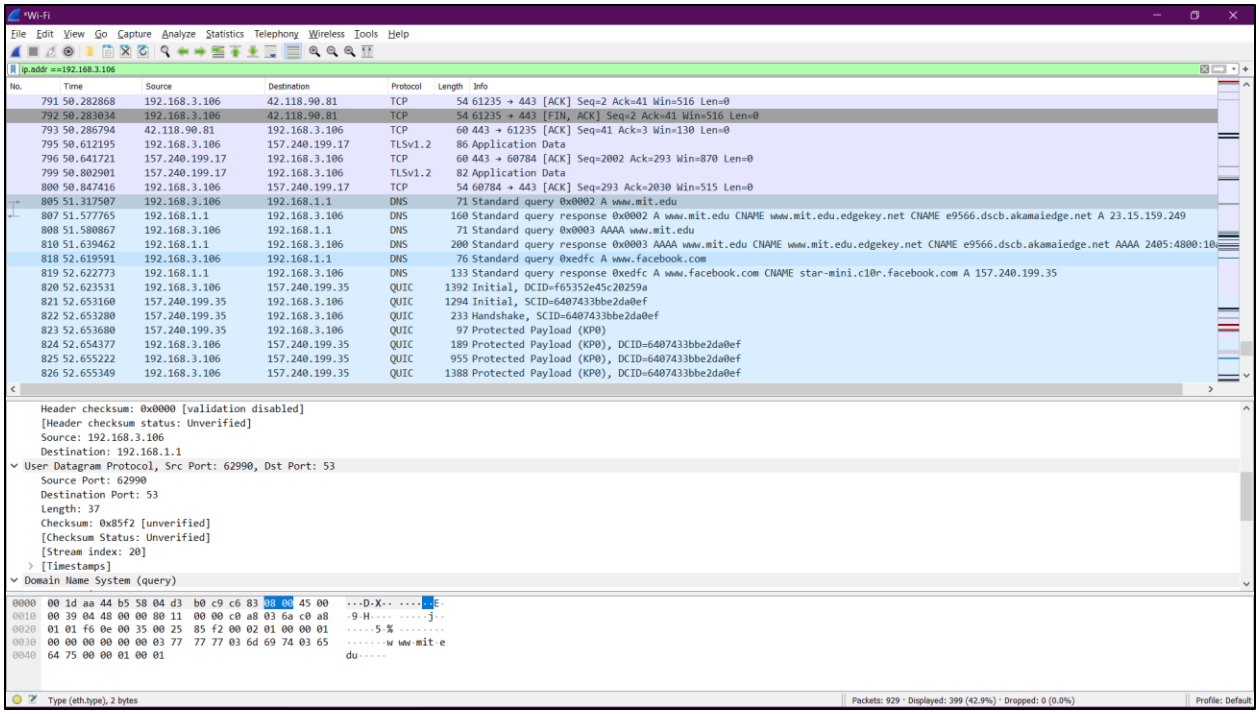
Question 14. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

ANSWER



Question 15. Provide a screenshot.

ANSWER


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr ==192.168.3.106
No. Time Source Destination Protocol Length Info
791 50.282868 192.168.3.106 42.118.90.81 TCP 54 61235 → 443 [ACK] Seq=2 Ack=41 Win=516 Len=0
792 50.283034 192.168.3.106 42.118.90.81 TCP 54 61235 → 443 [FIN, ACK] Seq=2 Ack=41 Win=516 Len=0
793 50.286794 42.118.90.81 192.168.3.106 TCP 60 443 → 61235 [ACK] Seq=41 Ack=3 Win=130 Len=0
795 50.612195 192.168.3.106 157.240.199.17 TLSv1.2 86 Application Data
796 50.641721 157.240.199.17 192.168.3.106 TCP 60 443 → 60784 [ACK] Seq=2002 Ack=293 Win=870 Len=0
799 50.802901 157.240.199.17 192.168.3.106 TLSv1.2 82 Application Data
800 50.847416 192.168.3.106 157.240.199.17 TCP 54 60784 → 443 [ACK] Seq=293 Ack=2030 Win=515 Len=0
805 51.317507 192.168.3.106 192.168.1.1 DNS 71 Standard query 0x0002 A www.mit.edu
807 51.577765 192.168.1.1 192.168.3.106 DNS 160 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.15.159.249
808 51.580867 192.168.3.106 192.168.1.1 DNS 71 Standard query 0x0003 AAAA www.mit.edu
810 51.639462 192.168.1.1 192.168.3.106 DNS 200 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2405:4800:10
818 52.619591 192.168.3.106 192.168.1.1 DNS 76 Standard query 0xedfc A www.facebook.com
819 52.622773 192.168.1.1 192.168.3.106 DNS 133 Standard query response 0xedfc A www.facebook.com CNAME star-mini.c10r.facebook.com A 157.240.199.35
820 52.623531 192.168.3.106 157.240.199.35 QUIC 1392 Initial, DCID=f65352e45c20259a
821 52.653160 157.240.199.35 192.168.3.106 QUIC 1294 Initial, SCID=6407433bbe2da0ef
822 52.653280 157.240.199.35 192.168.3.106 QUIC 233 Handshake, SCID=6407433bbe2da0ef
823 52.653680 157.240.199.35 192.168.3.106 QUIC 97 Protected Payload (KP0)
824 52.654377 192.168.3.106 157.240.199.35 QUIC 189 Protected Payload (KP0), DCID=6407433bbe2da0ef
825 52.655222 192.168.3.106 157.240.199.35 QUIC 955 Protected Payload (KP0), DCID=6407433bbe2da0ef
826 52.655349 192.168.3.106 157.240.199.35 QUIC 1388 Protected Payload (KP0), DCID=6407433bbe2da0ef
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.3.106
Destination: 192.168.1.1
User Datagram Protocol, Src Port: 62990, Dst Port: 53
Source Port: 62990
Destination Port: 53
Length: 37
Checksum: 0x85f2 [unverified]
[Checksum Status: Unverified]
[Stream index: 20]
[Timestamps]
Domain Name System (query)
0000 00 1d aa 44 b5 58 04 d3 b0 c9 c6 83 08 00 45 00 ···D·X·· ····· ··E·
0010 00 39 04 48 00 00 80 11 00 00 c0 a8 03 6a c0 a8 ·9·H···· ·····j··
0020 01 01 f6 0e 00 35 00 25 85 f2 00 02 01 00 00 01 ·····5·% ·····
0030 00 00 00 00 00 00 03 77 77 77 03 6d 69 74 03 65 ·····w www·mit·e
0040 64 75 00 00 01 00 01 du·····
Type (eth.type), 2 bytes
Packets: 929 · Displayed: 399 (42.9%) · Dropped: 0 (0.0%)
Profile: Default