

DNS Homework

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

Ans : 120.107.179.225.

```
C:\Users\user>nslookup ncue.edu.tw
伺服器:  dns.google
Address:  8.8.8.8

未經授權的回答:
名稱:      ncue.edu.tw
Address:   120.107.179.225
```

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

Ans : dns.ncue.edu.tw.

```
C:\Users\user>nslookup -type=NS www.ncue.edu.tw
伺服器:  dns.google
Address:  8.8.8.8

ncue.edu.tw
    primary name server = dns.ncue.edu.tw
    responsible mail addr = postmaster.dns.ncue.edu.tw
    serial = 2021111015
    refresh = 60 (1 min)
    retry = 30 (30 secs)
    expire = 3600000 (41 days 16 hours)
    default TTL = 3600 (1 hour)
```

3. 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?

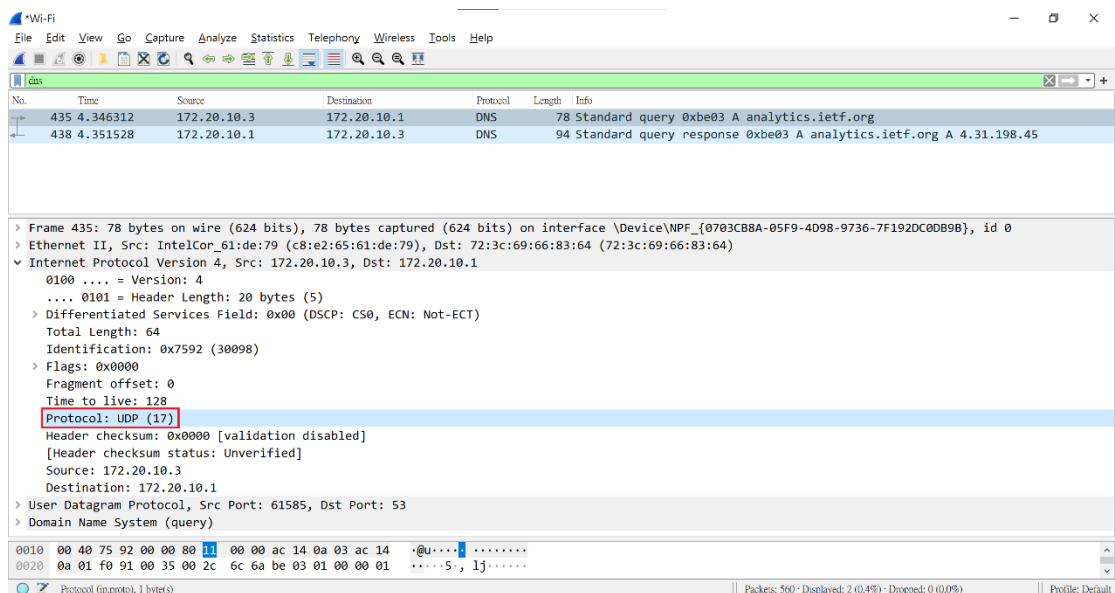
Ans : The IP address for the DNS server if queried for the Yahoo! mail server IP address is 119.161.14.17.

```
C:\Users\user>nslookup www.ncue.edu.tw mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
伺服器: UnKnown
Address: 119.161.14.17

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** 對 UnKnown 的要求逾時
```

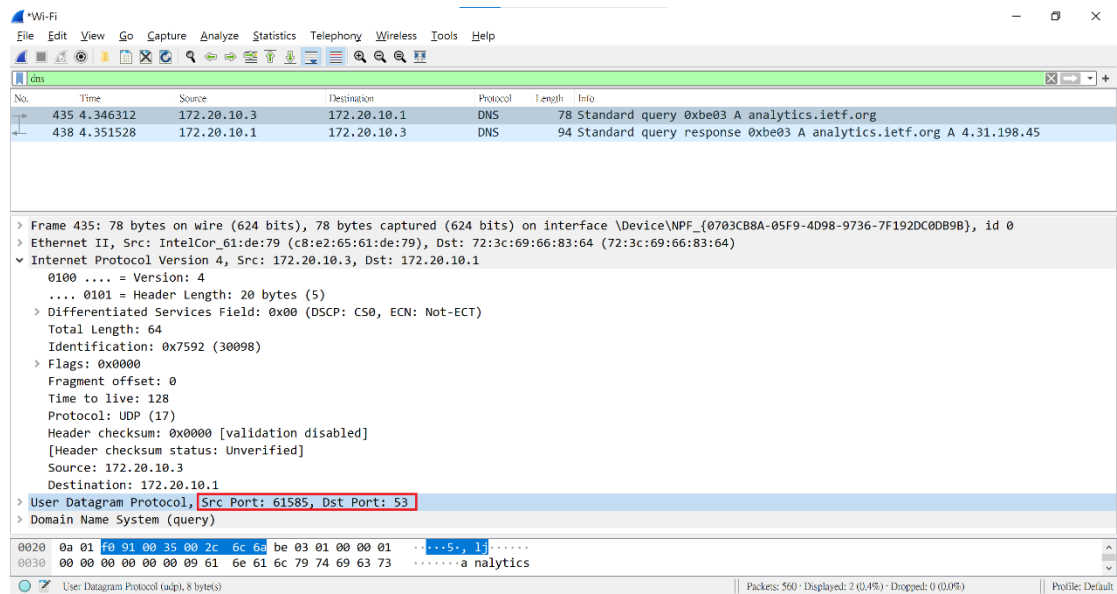
4. Locate the DNS query and response messages. Are then sent over UDP or TCP?

Ans : UDP.



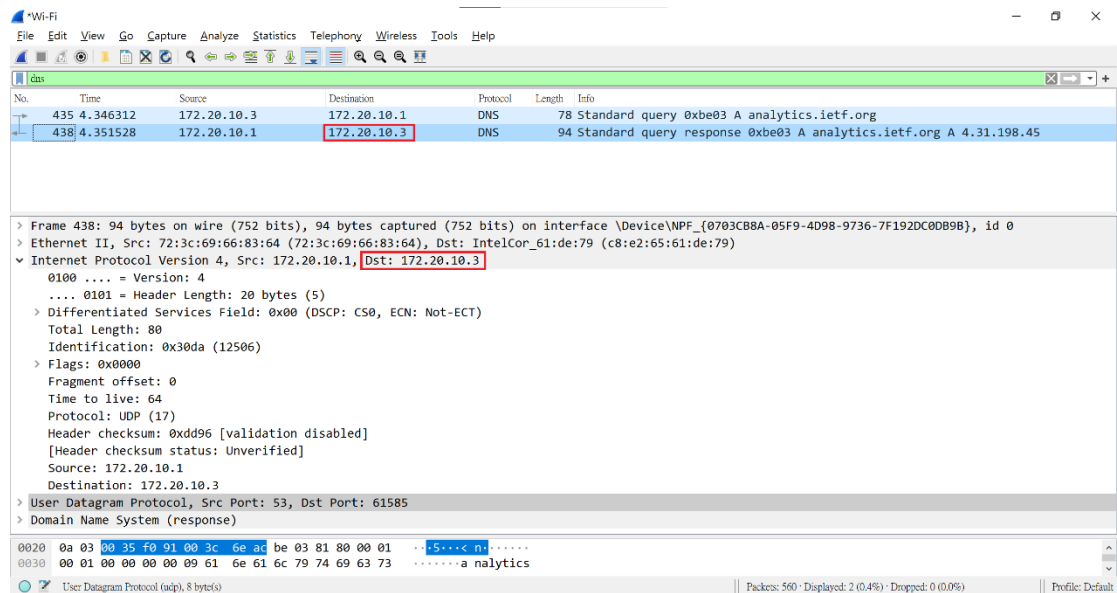
5. What is the destination port for the DNS query message? What is the source port of DNS response message?

Ans : Source port: 61585, Destination port: 53.



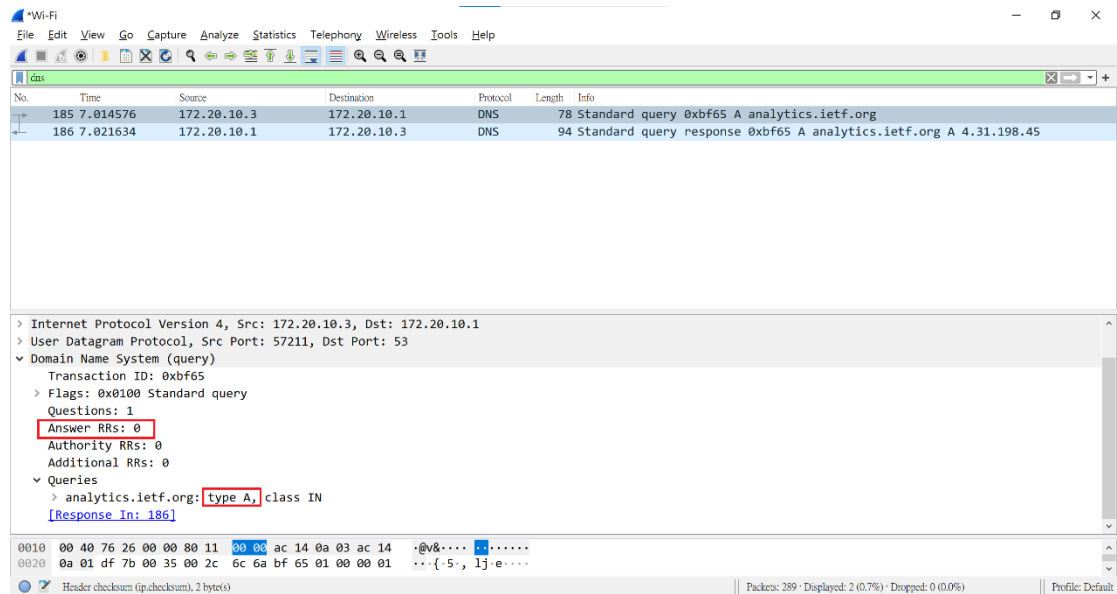
6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

Ans : First IP address is 172.20.10.3 the other is 172.20.10.1.



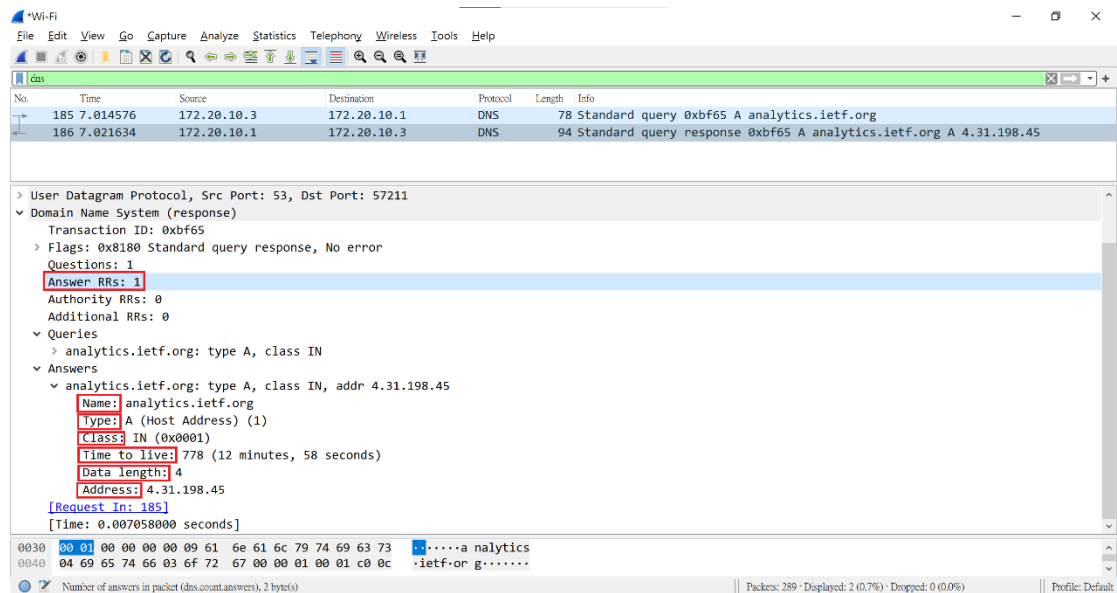
7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Ans : Type A, no answers.



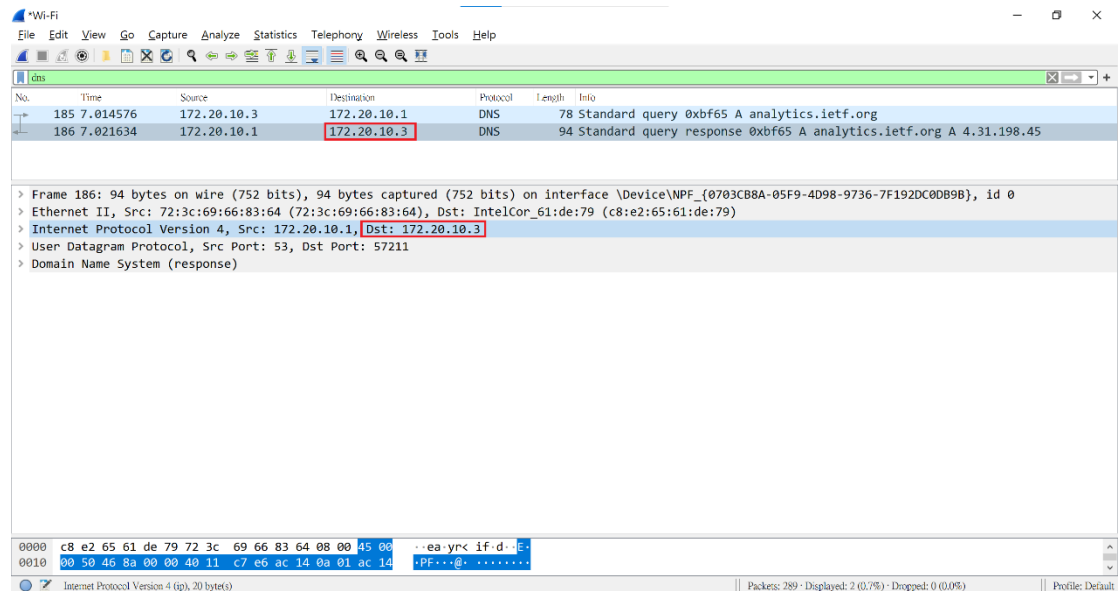
8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Ans : 1, Contain: Name, Type, Class, TTL(Time To Live) , Data Length , Address.



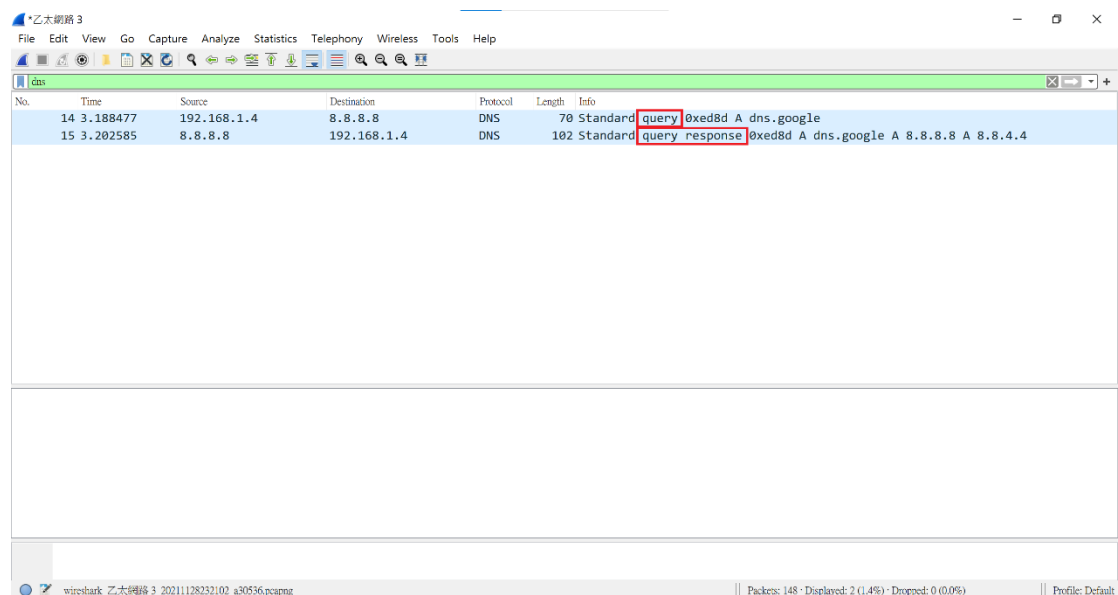
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Ans : 172.20.10.3.



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

Ans : No, only one queries. (注:此處我有換網路故 DNS server 不同)



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

Ans : Destination port “53” for the DNS query message.

Source port “53” of DNS response message.

The screenshot shows a Wireshark packet capture of a DNS query. The packet list pane displays several packets, with packet 32 selected. The packet details pane shows the structure of the packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). The UDP section shows the source port as 55701 and the destination port as 53. The packet bytes pane shows the raw data of the packet, with the destination port 53 highlighted in red.

No.	Time	Source	Destination	Protocol	Length	Info
32	2.954130	192.168.1.4	8.8.8.8	DNS	71	Standard query 0xebd6 A www.mit.edu
33	2.992128	8.8.8.8	192.168.1.4	DNS	160	Standard query response 0xebd6 A www.mit.edu CNAME www.mit.edu.edgekey.net...
34	2.994119	192.168.1.4	23.202.126.78	DNS	86	Standard query 0x0001 PTR 78.126.202.23.in-addr.arpa
62	5.003902	192.168.1.4	23.202.126.78	DNS	62	Standard query 0x0002 A on
69	7.007140	192.168.1.4	23.202.126.78	DNS	62	Standard query 0x0003 AAAA on

> Frame 32: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{8C44A92B-D7C1-432E-9A8D-28DFEF13B2B0}, id 0
> Ethernet II, Src: RealtekS_68:0c:c2 (00:e0:4c:68:0c:c2), Dst: Tp-LinkT_66:9d:c0 (68:ff:7b:66:9d:c0)
> Internet Protocol Version 4, Src: 192.168.1.4, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 55701, Dst Port: 53
> Domain Name System (query)

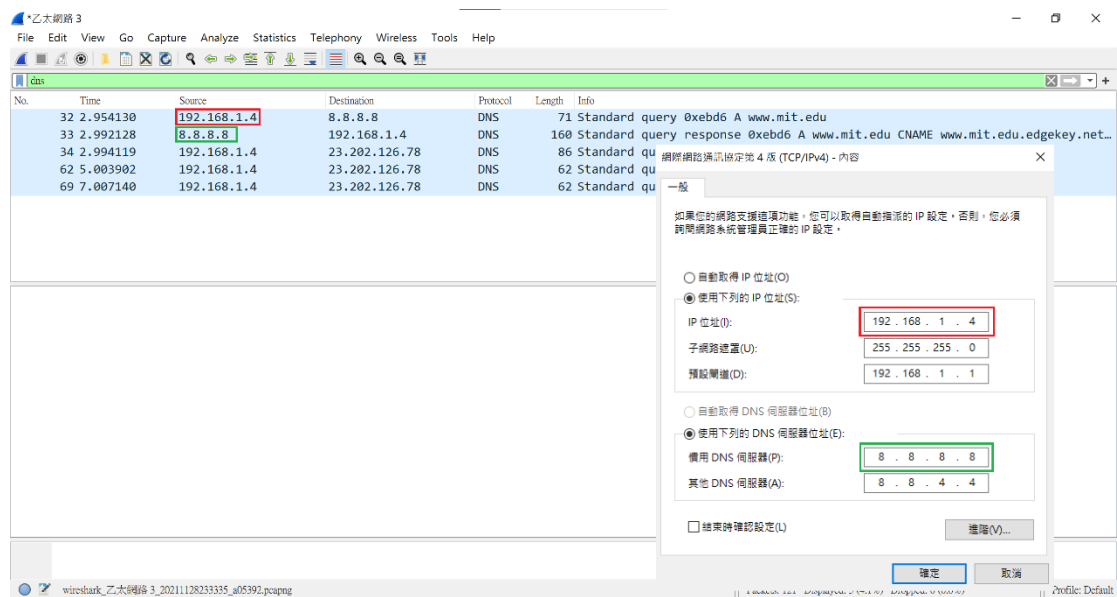
The screenshot shows a Wireshark packet capture of a DNS response. The packet list pane displays several packets, with packet 33 selected. The packet details pane shows the structure of the packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (response). The UDP section shows the source port as 53 and the destination port as 55701. The packet bytes pane shows the raw data of the packet, with the source port 53 highlighted in red.

No.	Time	Source	Destination	Protocol	Length	Info
32	2.954130	192.168.1.4	8.8.8.8	DNS	71	Standard query 0xebd6 A www.mit.edu
33	2.992128	8.8.8.8	192.168.1.4	DNS	160	Standard query response 0xebd6 A www.mit.edu CNAME www.mit.edu.edgekey.net...
34	2.994119	192.168.1.4	23.202.126.78	DNS	86	Standard query 0x0001 PTR 78.126.202.23.in-addr.arpa
62	5.003902	192.168.1.4	23.202.126.78	DNS	62	Standard query 0x0002 A on
69	7.007140	192.168.1.4	23.202.126.78	DNS	62	Standard query 0x0003 AAAA on

> Frame 33: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{8C44A92B-D7C1-432E-9A8D-28DFEF13B2B0}, id 0
> Ethernet II, Src: Tp-LinkT_66:9d:c0 (68:ff:7b:66:9d:c0), Dst: RealtekS_68:0c:c2 (00:e0:4c:68:0c:c2)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.4
> User Datagram Protocol, Src Port: 53, Dst Port: 55701
> Domain Name System (response)

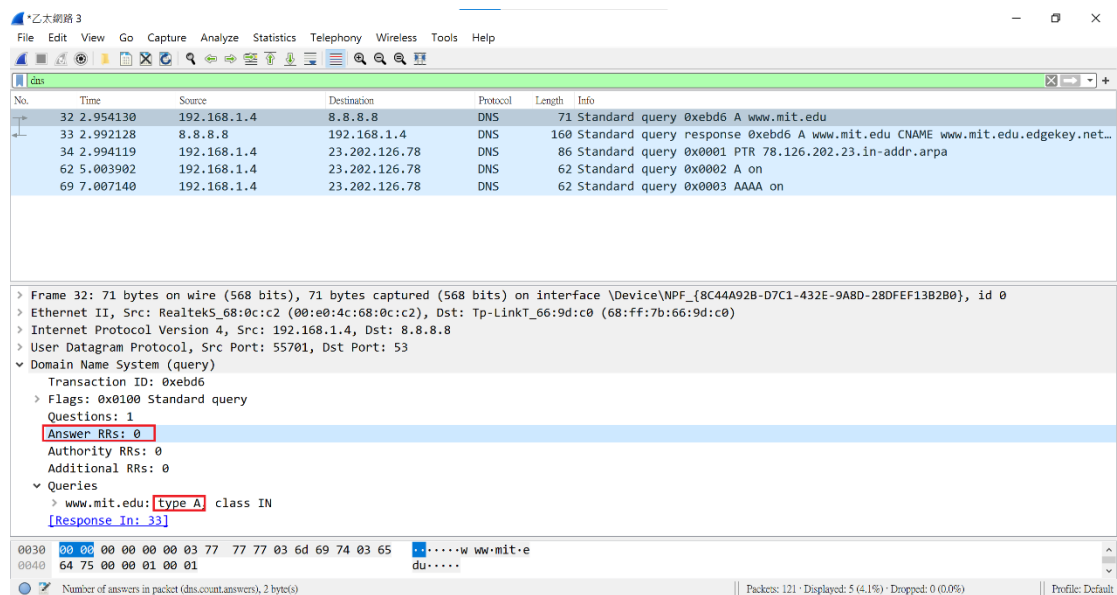
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Ans : 192.168.1.4, yes.



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

Ans : Type A, no answer.



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

Ans : 3, Contain: Type, Class, TTL(Time To Live), Data Length, (Address or CNAME).

Wireshark packet capture showing a DNS response message. The packet list shows a standard query response for www.mit.edu. The packet details pane shows the domain name system response with 3 answer RRs. The packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
32	2.954130	192.168.1.4	8.8.8.8	DNS	71	Standard query 0xebd6 A www.mit.edu
33	2.992128	8.8.8.8	192.168.1.4	DNS	160	Standard query response 0xebd6 A www.mit.edu CNAME www.mit.edu.edgekey.net...
34	2.994119	192.168.1.4	23.202.126.78	DNS	86	Standard query 0x0001 PTR 78.126.202.23.in-addr.arpa
62	5.003902	192.168.1.4	23.202.126.78	DNS	62	Standard query 0x0002 A on
69	7.007140	192.168.1.4	23.202.126.78	DNS	62	Standard query 0x0003 AAAA on

Frame 33: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{8C4A92B-D7C1-432E-9A8D-28DFEF13B2B0}, id 0
 Ethernet II, Src: Tp-LinkT_66:9d:c0 (68:ff:7b:66:9d:c0), Dst: RealtekS_68:0c:c2 (00:e0:4c:68:0c:c2)
 Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.4
 User Datagram Protocol, Src Port: 53, Dst Port: 55701
 Domain Name System (response)
 Transaction ID: 0xebd6
 Flags: 0x8180 Standard query response, No error
 Questions: 1
 Answer RRs: 3
 Authority RRs: 0
 Additional RRs: 0
 Queries
 > www.mit.edu: type A, class IN
 Answers
 > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
 > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
 > e9566.dscb.akamaiedge.net: type A, class IN, addr 23.202.126.78
 [Request In: 32]

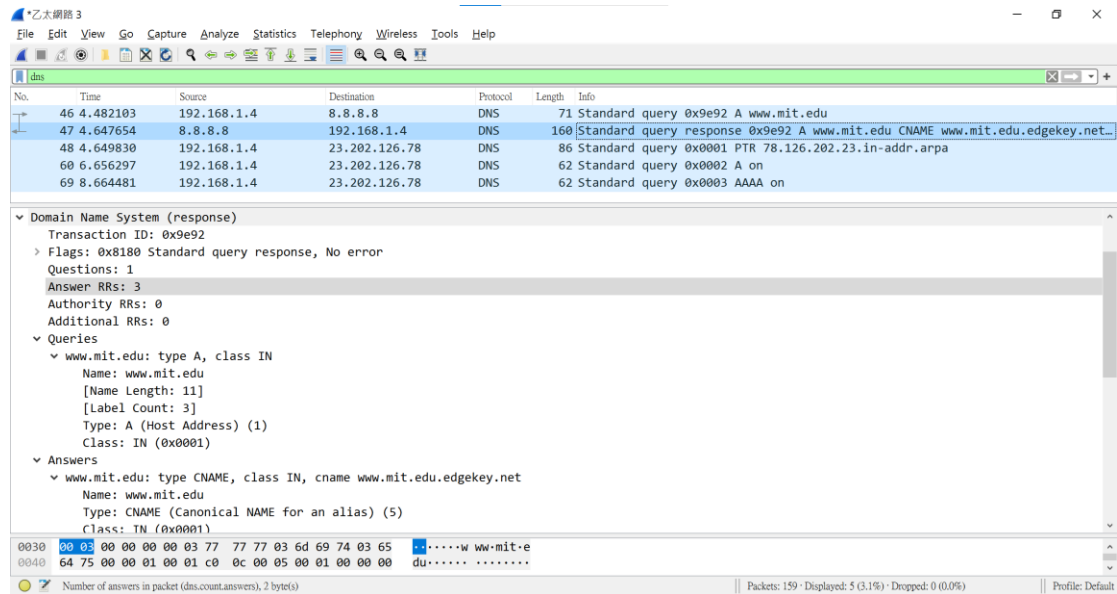
Wireshark packet capture showing the details of the DNS response message. The packet details pane shows the domain name system response with 3 answer RRs. The packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
32	2.954130	192.168.1.4	8.8.8.8	DNS	71	Standard query 0xebd6 A www.mit.edu
33	2.992128	8.8.8.8	192.168.1.4	DNS	160	Standard query response 0xebd6 A www.mit.edu CNAME www.mit.edu.edgeke...

Answers
 > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
 Name: www.mit.edu
 Type: CNAME (Canonical NAME for an alias) (5)
 Class: IN (0x0001)
 Time to live: 165 (2 minutes, 45 seconds)
 Data length: 25
 CNAME: www.mit.edu.edgekey.net
 > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
 Name: www.mit.edu.edgekey.net
 Type: CNAME (Canonical NAME for an alias) (5)
 Class: IN (0x0001)
 Time to live: 60 (1 minute)
 Data length: 24
 CNAME: e9566.dscb.akamaiedge.net
 > e9566.dscb.akamaiedge.net: type A, class IN, addr 23.202.126.78
 Name: e9566.dscb.akamaiedge.net
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 20 (20 seconds)
 Data length: 4
 Address: 23.202.126.78

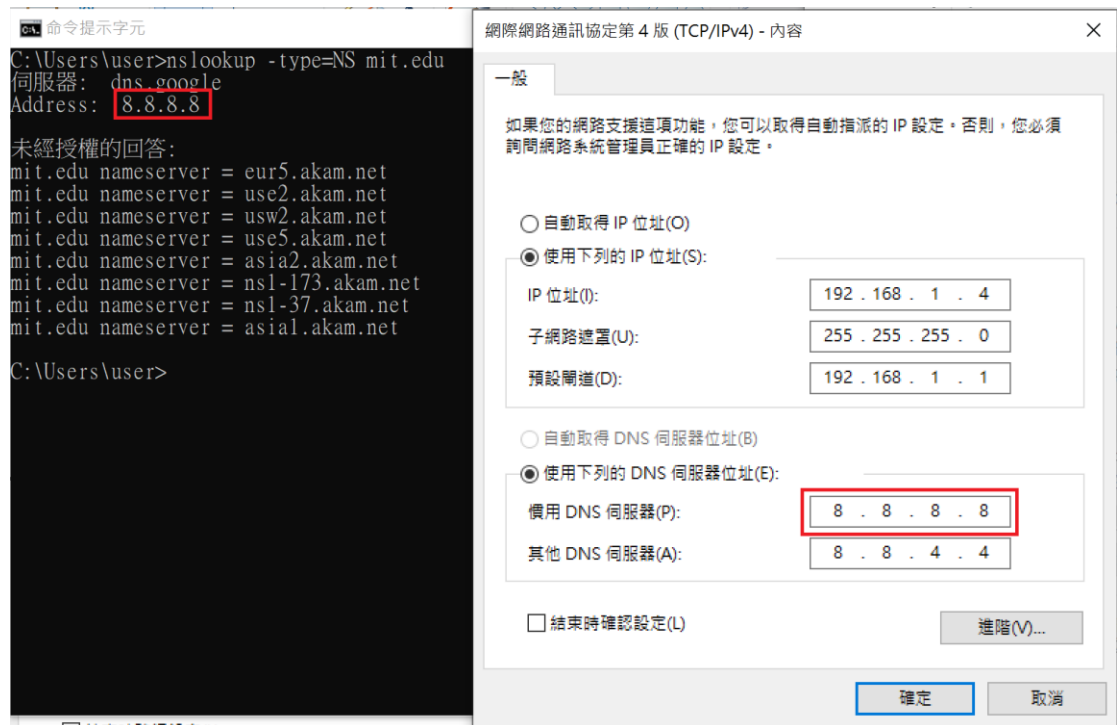
15. Provide a screenshot.

Ans : As following.



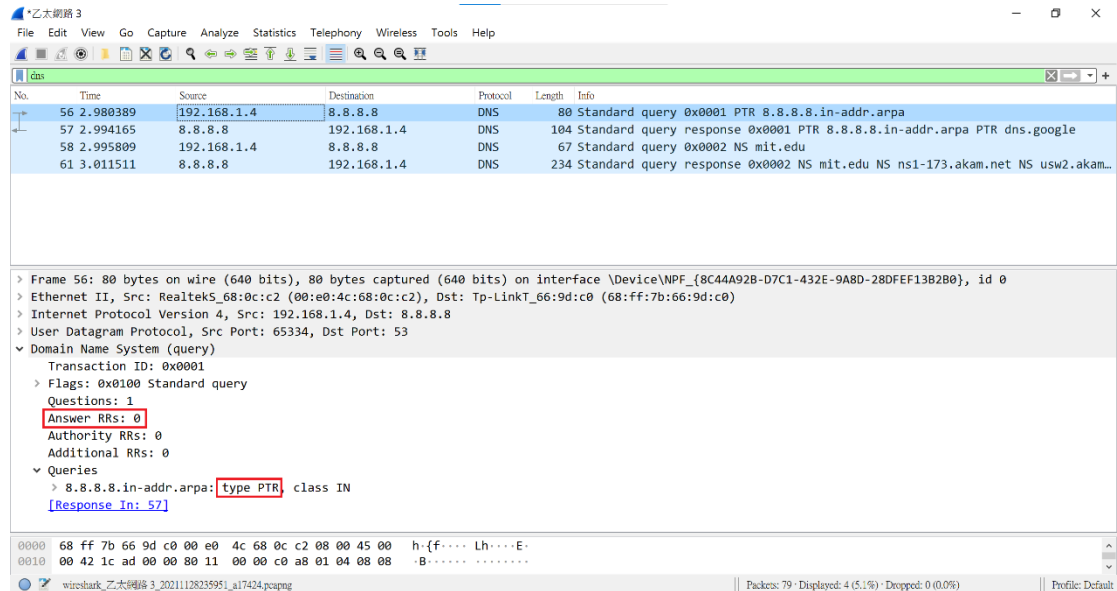
16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Ans : 8.8.8.8, Yes.



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

Ans : Respectively Type PTR and Type NS, then the two query messages are not answer.



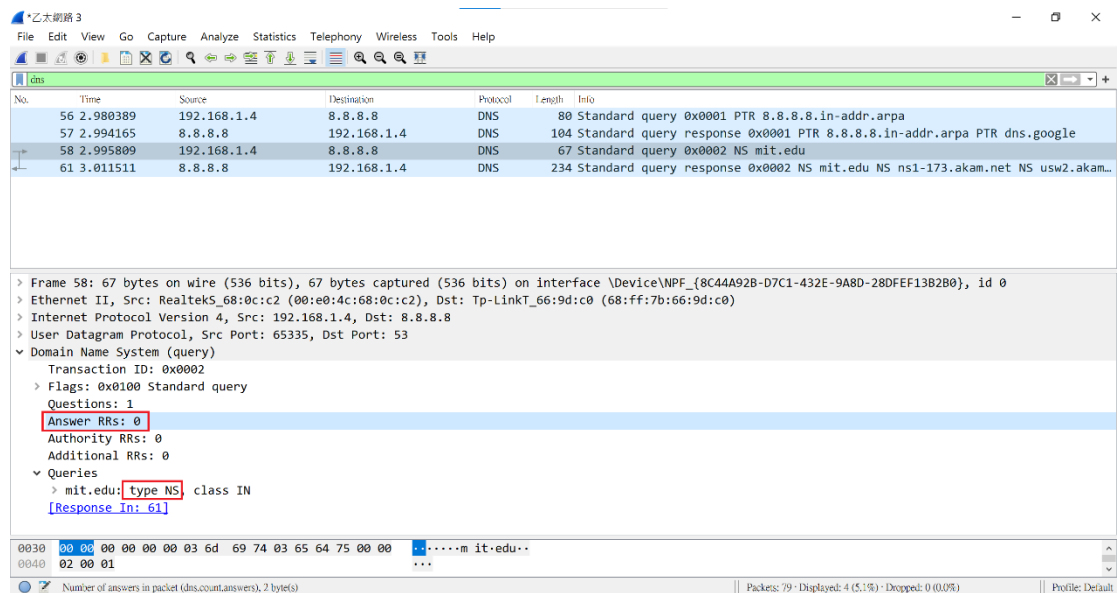
The screenshot shows a Wireshark capture of a DNS query. The packet list pane displays four packets:

No.	Time	Source	Destination	Protocol	Length	Info
56	2.980389	192.168.1.4	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
57	2.994165	8.8.8.8	192.168.1.4	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
58	2.995809	192.168.1.4	8.8.8.8	DNS	67	Standard query 0x0002 NS mit.edu
61	3.011511	8.8.8.8	192.168.1.4	DNS	234	Standard query response 0x0002 NS mit.edu NS ns1-173.akam.net NS usw2.akam...

The packet details pane for packet 56 shows the following information:

- Frame 56: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{8C44A92B-D7C1-432E-9A8D-28DFF13B2B0}, id 0
- Ethernet II, Src: RealtekS_68:0c:c2 (00:e0:4c:68:0c:c2), Dst: Tp-LinkT_66:9d:c0 (68:ff:7b:66:9d:c0)
- Internet Protocol Version 4, Src: 192.168.1.4, Dst: 8.8.8.8
- User Datagram Protocol, Src Port: 65334, Dst Port: 53
- Domain Name System (query)
 - Transaction ID: 0x0001
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - 8.8.8.8.in-addr.arpa: type PTR, class IN

The packet bytes pane shows the raw data of the DNS query.



The screenshot shows a Wireshark capture of a DNS query. The packet list pane displays four packets:

No.	Time	Source	Destination	Protocol	Length	Info
56	2.980389	192.168.1.4	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
57	2.994165	8.8.8.8	192.168.1.4	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
58	2.995809	192.168.1.4	8.8.8.8	DNS	67	Standard query 0x0002 NS mit.edu
61	3.011511	8.8.8.8	192.168.1.4	DNS	234	Standard query response 0x0002 NS mit.edu NS ns1-173.akam.net NS usw2.akam...

The packet details pane for packet 58 shows the following information:

- Frame 58: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{8C44A92B-D7C1-432E-9A8D-28DFF13B2B0}, id 0
- Ethernet II, Src: RealtekS_68:0c:c2 (00:e0:4c:68:0c:c2), Dst: Tp-LinkT_66:9d:c0 (68:ff:7b:66:9d:c0)
- Internet Protocol Version 4, Src: 192.168.1.4, Dst: 8.8.8.8
- User Datagram Protocol, Src Port: 65335, Dst Port: 53
- Domain Name System (query)
 - Transaction ID: 0x0002
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - mit.edu: type NS, class IN

The packet bytes pane shows the raw data of the DNS query.

18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?

Ans :

1. ns1-173.akam.net, 2. usw2.akam.net, 3. eur5.akam.net.
4. use5.akam.net, 5. asia2.akam.net, 6. asia1.akam.net
7. use2.akam.net, 8. ns1-37.akam.net

No, I can't seeing IP address of the MIT nameservers.

I only can seeing: Name, Type, Class, TTL(Time To Live), Data Length, Name Server.

The screenshot shows a Wireshark packet capture of a DNS response message. The packet list pane shows four packets, with packet 61 selected. The packet details pane shows the structure of the DNS response, including the Answer RRs section which lists eight nameservers for mit.edu. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
56	2.980389	192.168.1.4	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
57	2.994165	8.8.8.8	192.168.1.4	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
58	2.995809	192.168.1.4	8.8.8.8	DNS	67	Standard query 0x0002 NS mit.edu
61	3.011511	8.8.8.8	192.168.1.4	DNS	234	Standard query response 0x0002 NS mit.edu NS ns1-173.akam.net NS usw2.akam...

Answer RRs: 8
Authority RRs: 0
Additional RRs: 0
Queries
 > mit.edu: type NS, class IN
Answers
 > mit.edu: type NS, class IN, ns ns1-173.akam.net
 > mit.edu: type NS, class IN, ns usw2.akam.net
 > mit.edu: type NS, class IN, ns eur5.akam.net
 > mit.edu: type NS, class IN, ns use5.akam.net
 > mit.edu: type NS, class IN, ns asia2.akam.net
 > mit.edu: type NS, class IN, ns asia1.akam.net
 > mit.edu: type NS, class IN, ns use2.akam.net
 > mit.edu: type NS, class IN, ns ns1-37.akam.net
[Request In: 58]

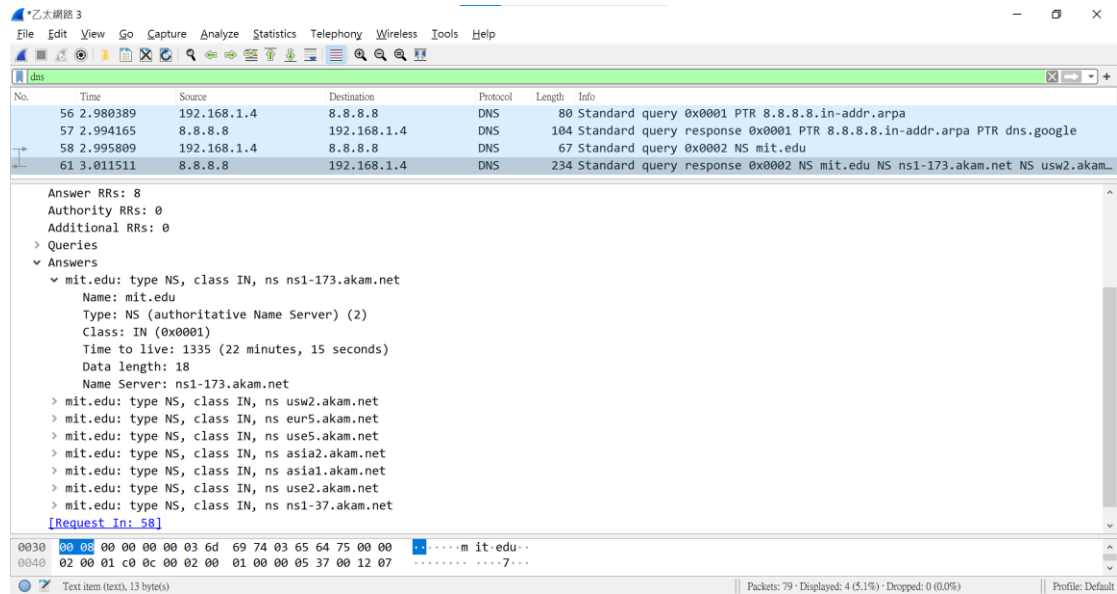
The screenshot shows a detailed view of the DNS response message for mit.edu. The packet details pane shows the structure of the DNS response, including the Answer RRs section which lists eight nameservers for mit.edu. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
56	2.980389	192.168.1.4	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
57	2.994165	8.8.8.8	192.168.1.4	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
58	2.995809	192.168.1.4	8.8.8.8	DNS	67	Standard query 0x0002 NS mit.edu
61	3.011511	8.8.8.8	192.168.1.4	DNS	234	Standard query response 0x0002 NS mit.edu NS ns1-173.akam.net NS usw2.akam...

Authority RRs: 0
Additional RRs: 0
Queries
 > mit.edu: type NS, class IN
Answers
 > mit.edu: type NS, class IN, ns ns1-173.akam.net
 Name: mit.edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 1335 (22 minutes, 15 seconds)
 Data length: 18
 Name Server: ns1-173.akam.net
 > mit.edu: type NS, class IN, ns usw2.akam.net
 > mit.edu: type NS, class IN, ns eur5.akam.net
 > mit.edu: type NS, class IN, ns use5.akam.net
 > mit.edu: type NS, class IN, ns asia2.akam.net
 > mit.edu: type NS, class IN, ns asia1.akam.net
 > mit.edu: type NS, class IN, ns use2.akam.net
 > mit.edu: type NS, class IN, ns ns1-37.akam.net
[Request In: 58]

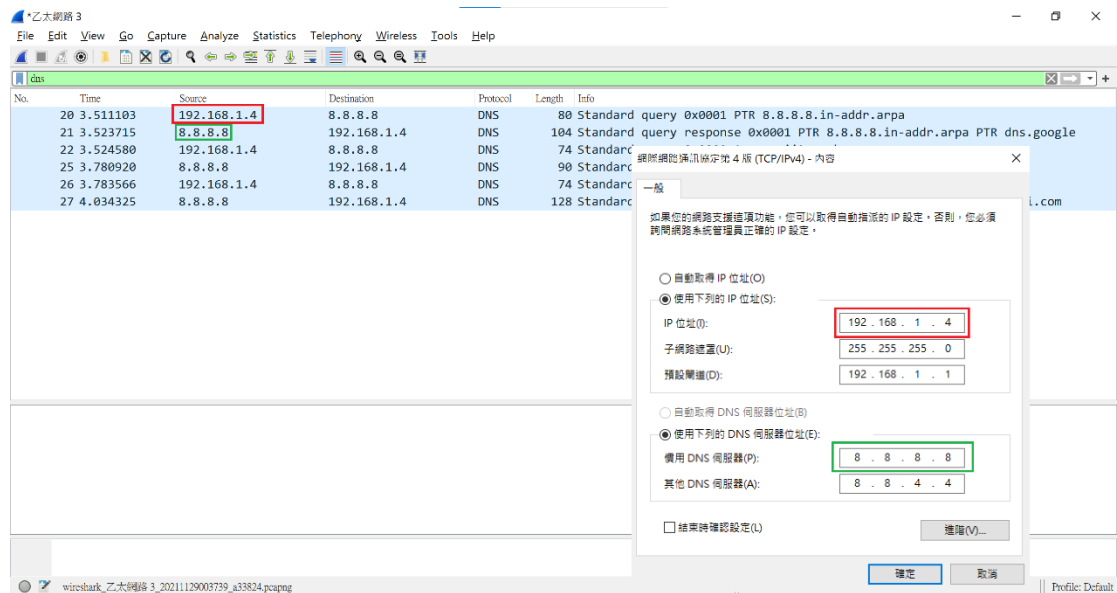
19. Provide a screenshot.

Ans : As following.



20. 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?

Ans : 192.168.1.4, Yes, because I'm not specify my DNS server, the server always are default.



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

Ans : Respectively Type PTR 、 Type A and Type AAAA, then the three query messages are not answer.

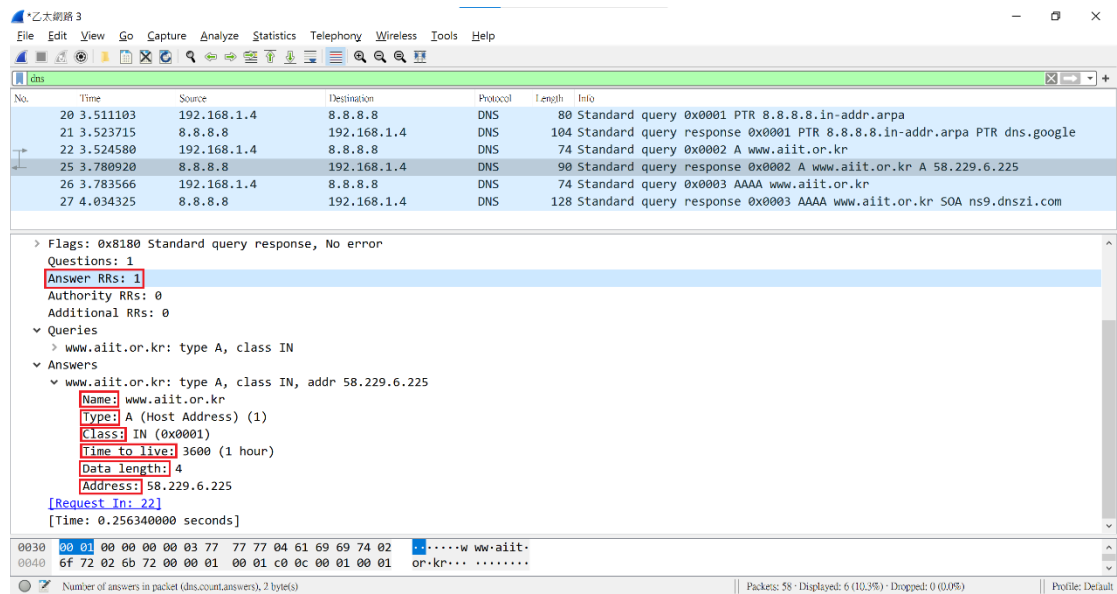
The image displays three screenshots of a Wireshark packet capture, specifically focusing on DNS queries. Each screenshot shows a list of packets at the top and a detailed view of a specific packet below.

- First Screenshot:** Shows packet 21 (No. 21, Time 3.523715, Source 8.8.8.8, Destination 192.168.1.4, Protocol DNS, Length 104). The detailed view shows a Domain Name System (query) transaction ID 0x0001. The query is for 8.8.8.8.in-addr.arpa with type PTR and class IN. The 'Answer RRs: 0' field is highlighted with a red box.
- Second Screenshot:** Shows packet 22 (No. 22, Time 3.524580, Source 8.8.8.8, Destination 192.168.1.4, Protocol DNS, Length 74). The detailed view shows a Domain Name System (query) transaction ID 0x0002. The query is for www.aiit.or.kr with type A and class IN. The 'type A' field is highlighted with a red box.
- Third Screenshot:** Shows packet 26 (No. 26, Time 3.783566, Source 192.168.1.4, Destination 8.8.8.8, Protocol DNS, Length 74). The detailed view shows a Domain Name System (query) transaction ID 0x0003. The query is for www.aiit.or.kr with type AAAA and class IN. The 'type AAAA' field is highlighted with a red box.

In all three screenshots, the 'Answer RRs: 0' field is consistently highlighted, indicating that these are query messages and not responses containing answers.

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

Ans : 1, Contain: Name Type, Class, TTL(Time To Live), Data Length, Address.



23. Provide a screenshot.

Ans : As following.

