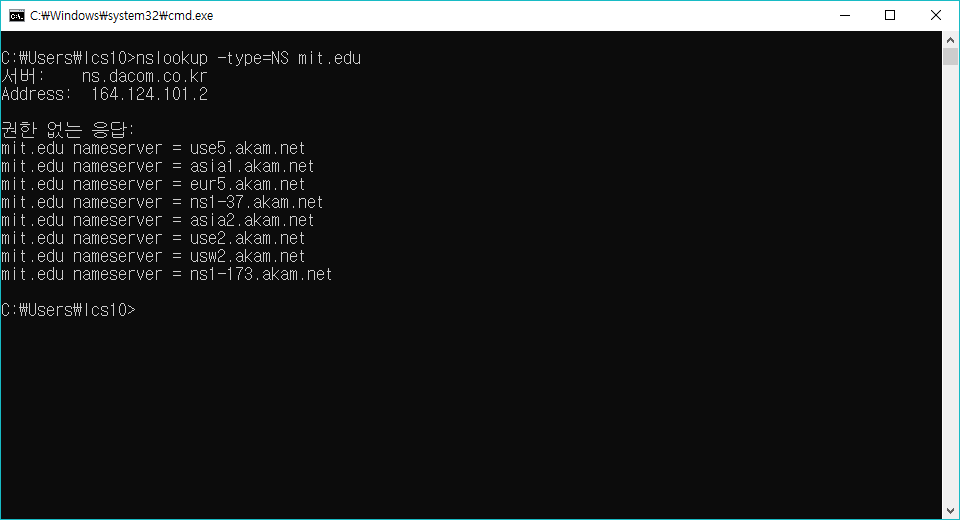
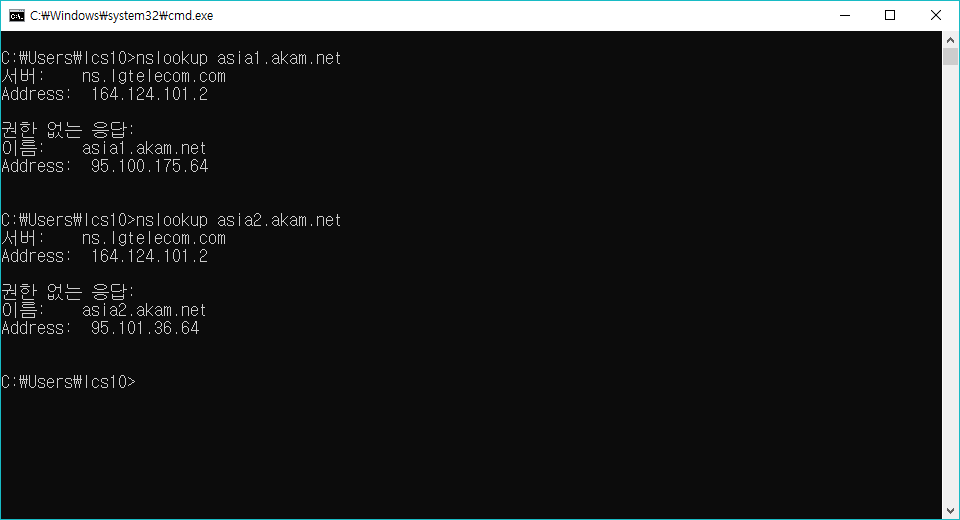
2.1 다음을 물음에 답을 하세요

1. nslookup을 실행하여, 아시아에 있는 웹 서버의 IP 주소를 얻어 보십시오.

해당 서버의 IP 주소는 무엇입니까?

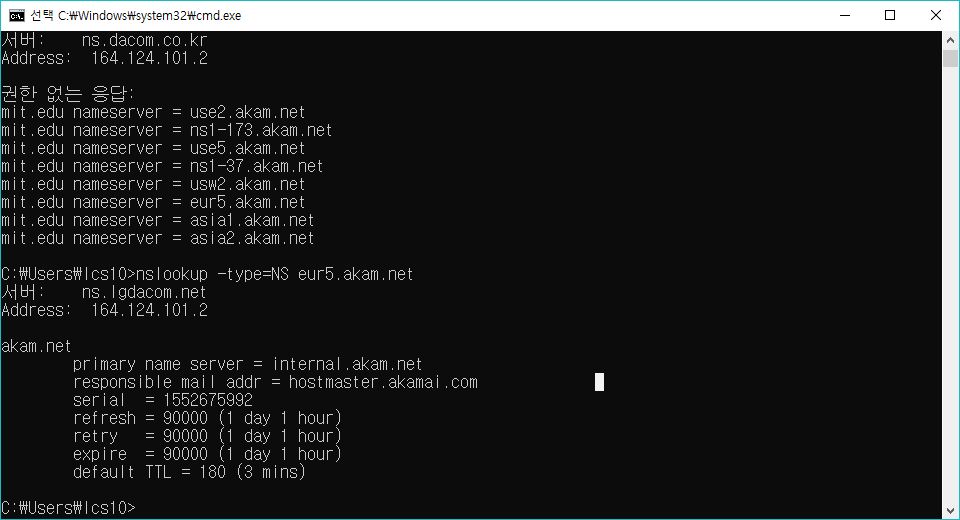
- 아시아에 있는 웹 서버의 주소는 2개가 존재하며 각각의 IP주소는





95.199.175.64, 95.101.36.64 입니다.

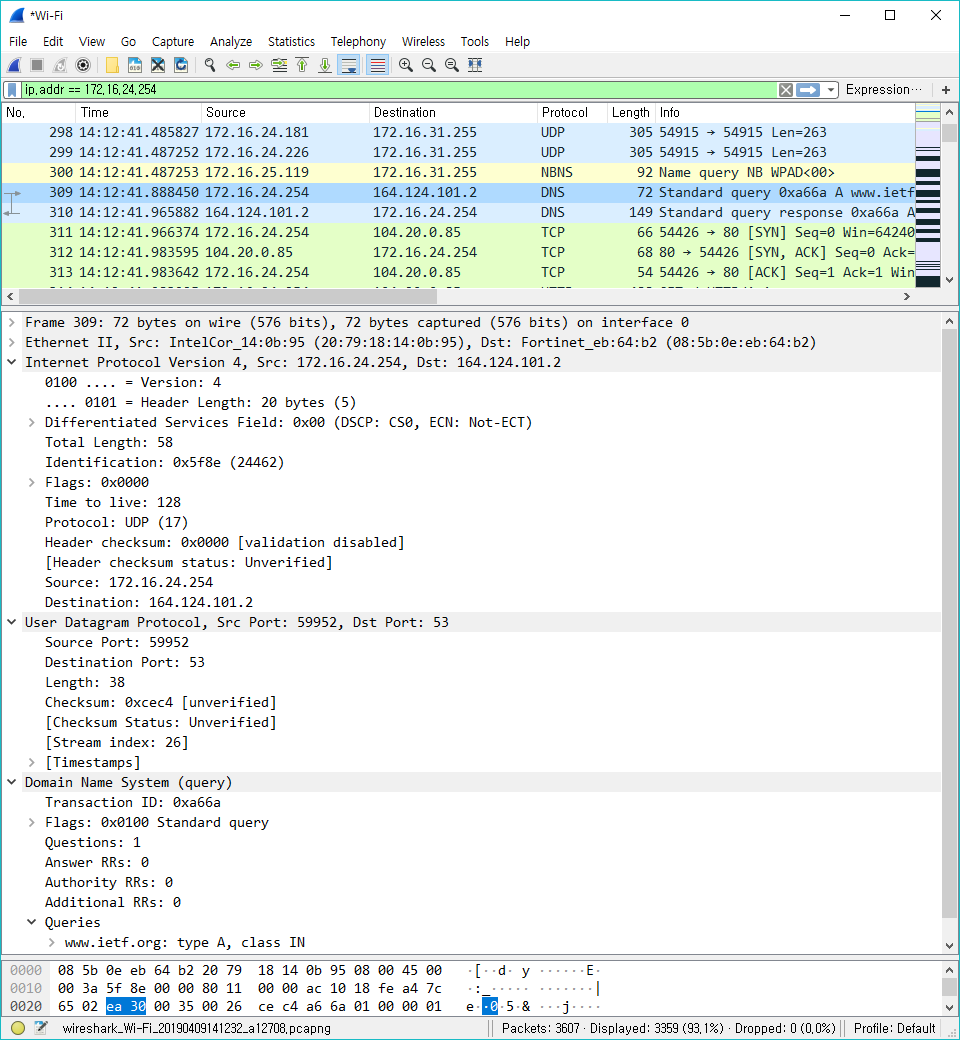
2. nslookup을 실행하여, 유럽에 있는 대학의 책임 (authoratative) DNS 서버를 확인해 보십시오.



**2.2 Wirechark에서의 DNS 동작 확인**

다음을 물음에 답을 하세요. 답을 할 경우 답변 시 사용한 패킷의 내용을 캡처해서 답과 함께 제출해야 합니다.

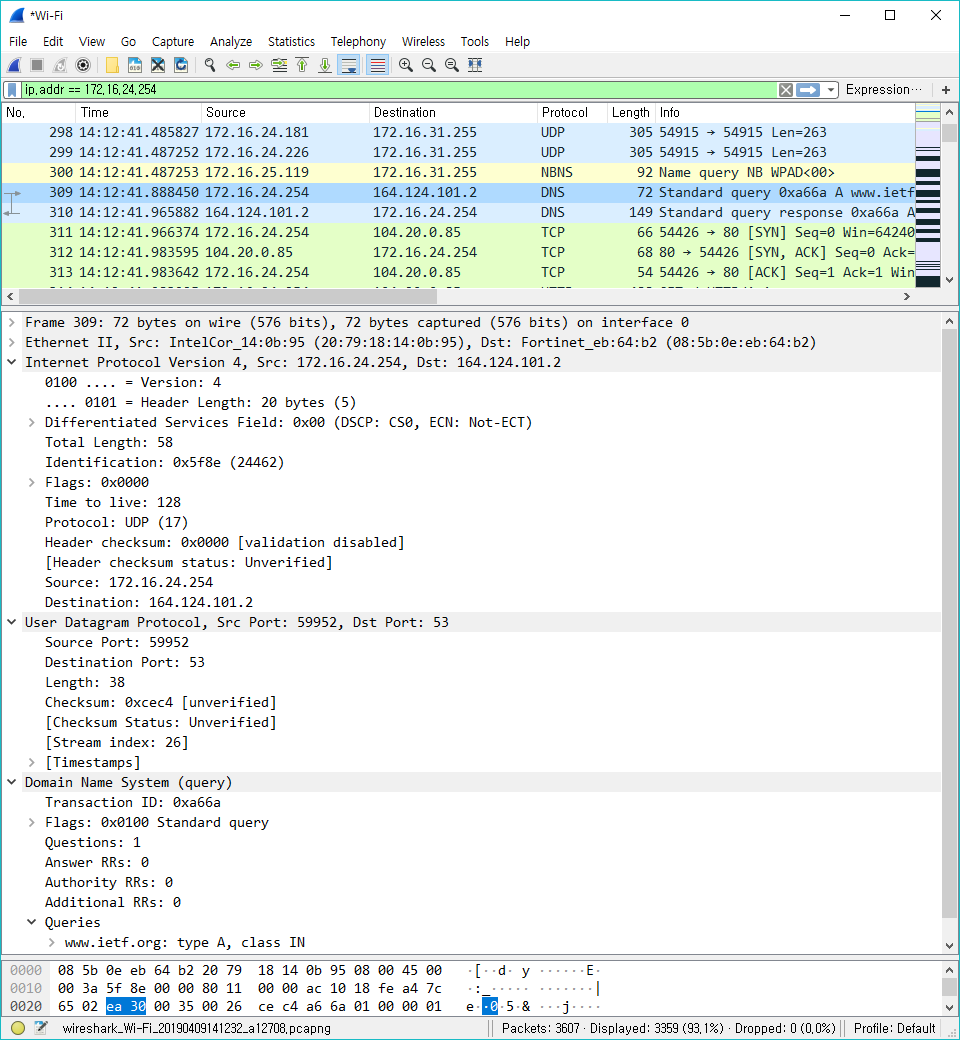
4. DNS 쿼리와 응답 메시지들을 찾습니다. UDP와 TCP 중 무엇으로 전송됐습니까?

UDP입니다.

5. DNS 쿼리 메시지의 대상 포트는 무엇입니까? DNS 응답 메시지의 소스 포트는 무엇입니까?

쿼리 메시지의 대상 포트 : 53

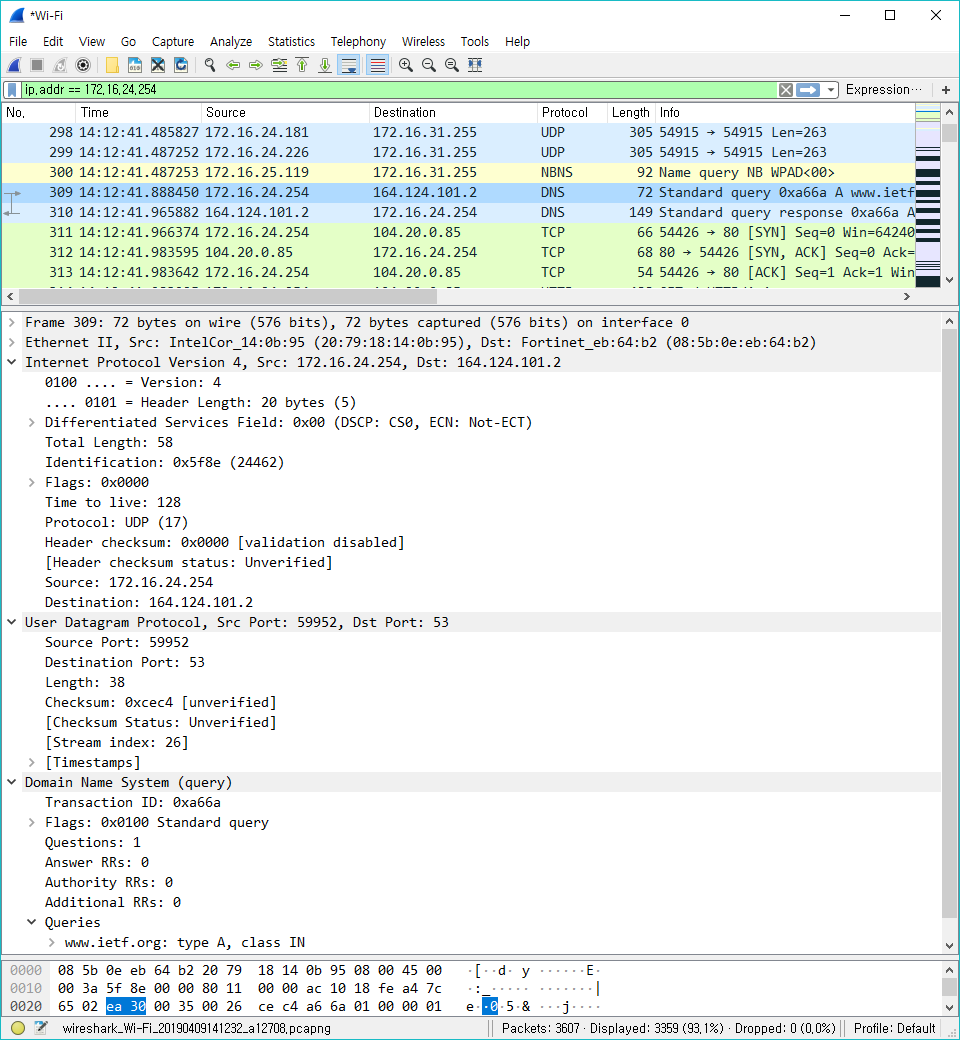
소스 포트 : 59952

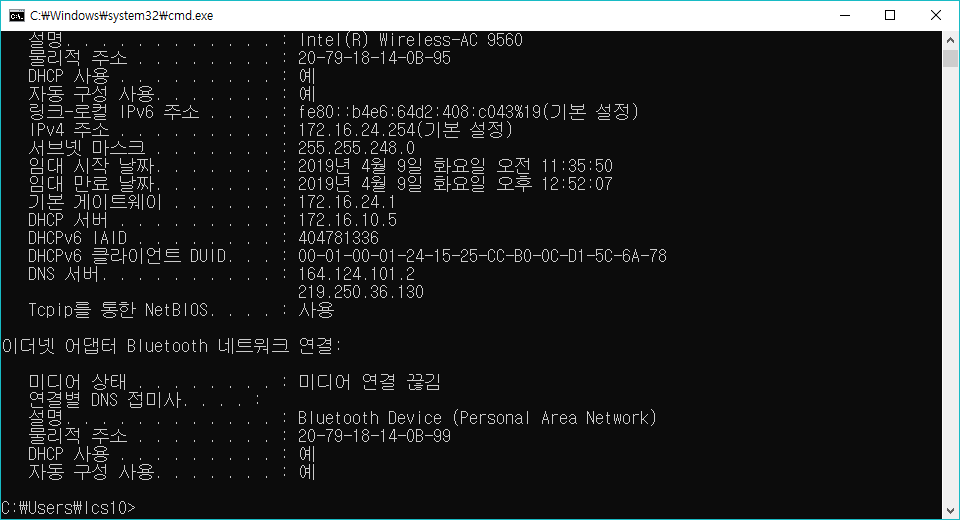


6. DNS 쿼리 메시지는 어떤 IP 주소로 전송됩니까? ipconfig를 사용하여 로컬 DNS 서버의 IP 주소를 확인하십시오. 두 IP 주소가 동일합니까?

전송하는 IP 주소 : 164.124.101.2

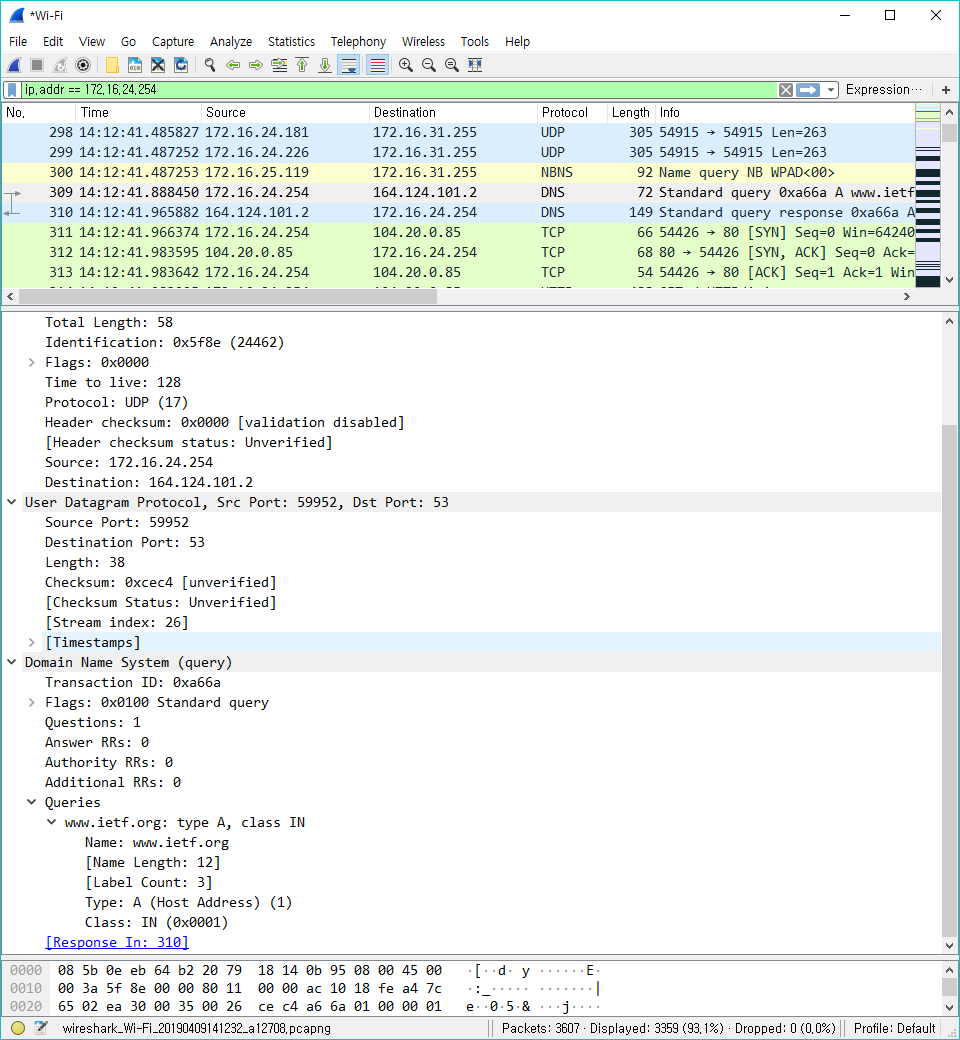
동일합니다.





7. DNS 쿼리 메시지를 확인하십시오. DNS 쿼리의 “타입”은 무엇입니까? 쿼리 메시지에 “답변”이 포함되어 있습니까?

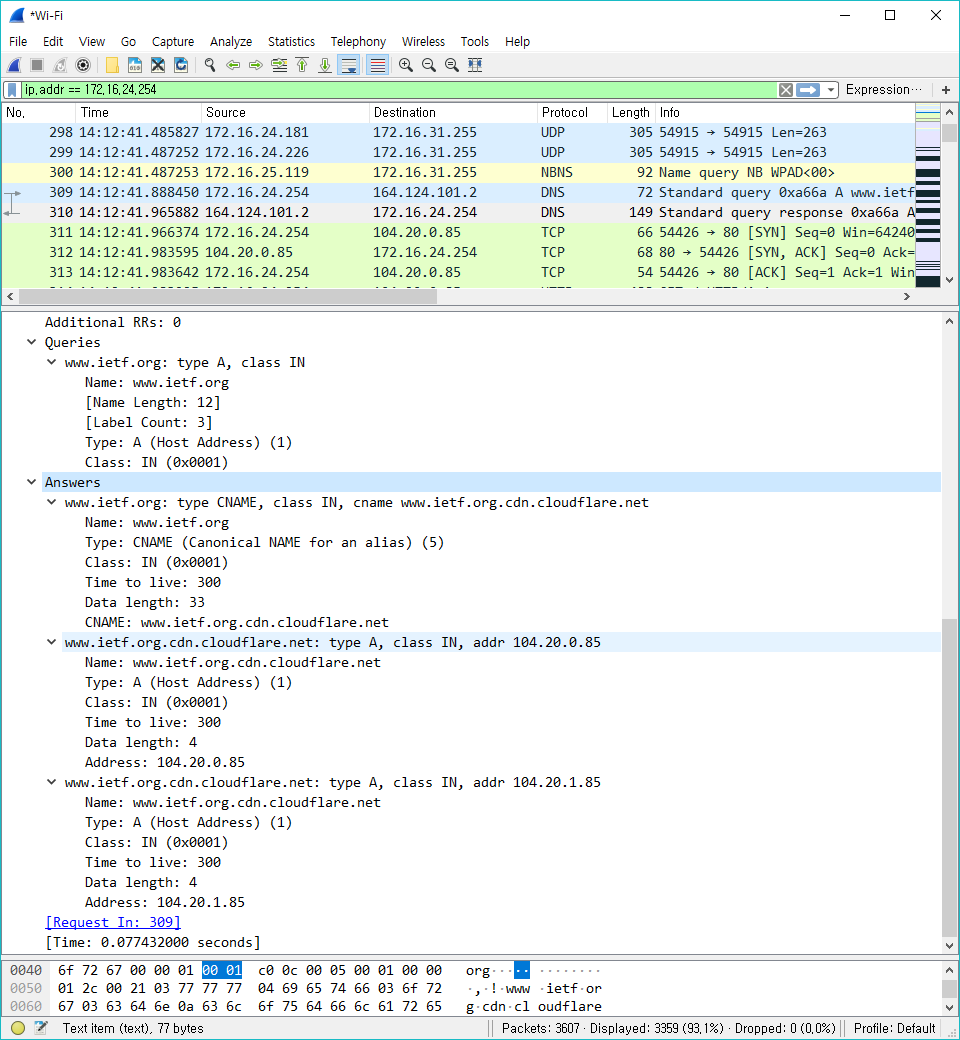
타입 : A, 쿼리 메시지에는 답변이 포함되어 있지 않습니다.



8. DNS 응답 메시지를 확인하십시오. 얼마나 많은 “답변”이 제공됩니까? 이 각각의 답변들은 무엇을 포함합니까?

3개의 답변이 포함됩니다.

Type, Class, TTL, Data length, CNAME, Address 등이 포함되어 있습니다

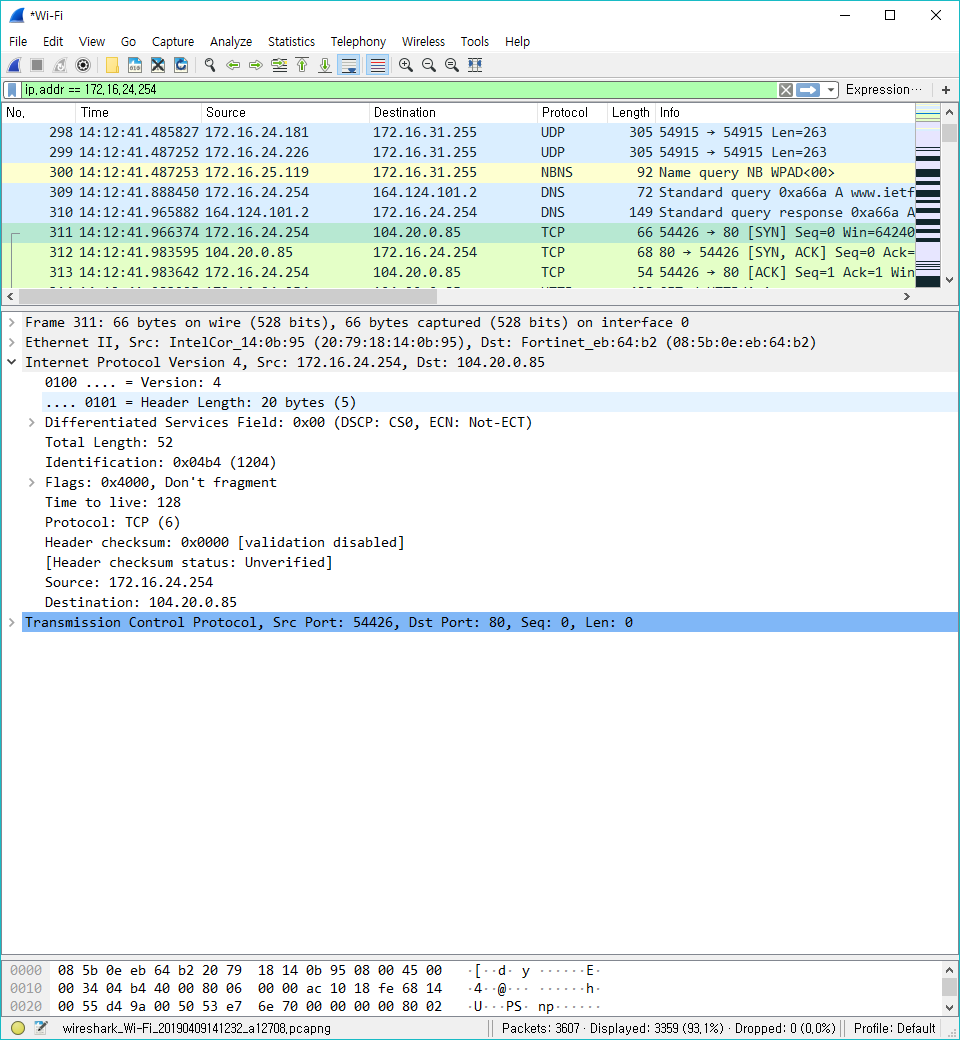
.

9. 호스트가 보낸 후속 TCP SYN 패킷을 고려하십시오. SYN 패킷의 대상 IP 주소가 DNS 응답 메시지에 제공된 IP 주소 중 하나와 일치합니까?

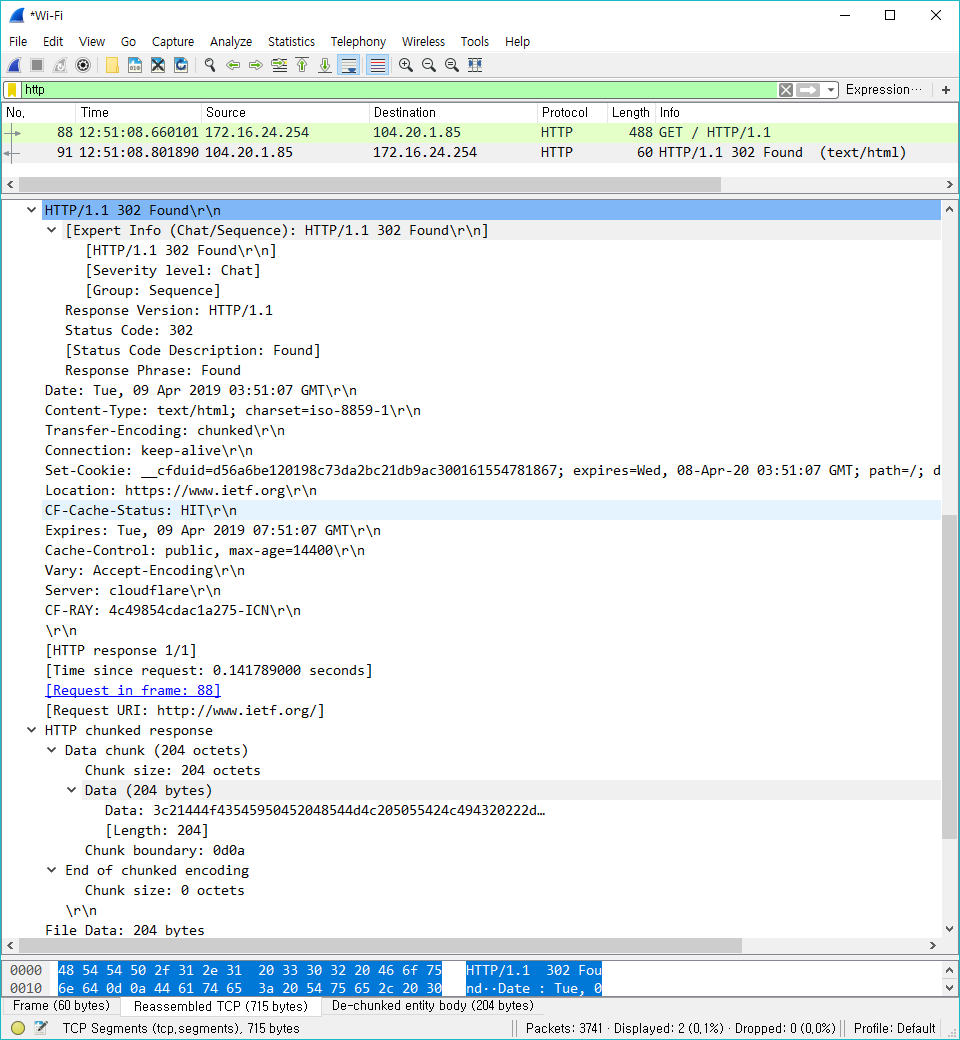
네 일치합니다.

8번 사진에 따르면 응답메시지에서 104.20.0.85, 104.20.1.85 두 IP를 제공하였으며

SYN 패킷의 목적지 IP는 104.20.0.85 입니다.

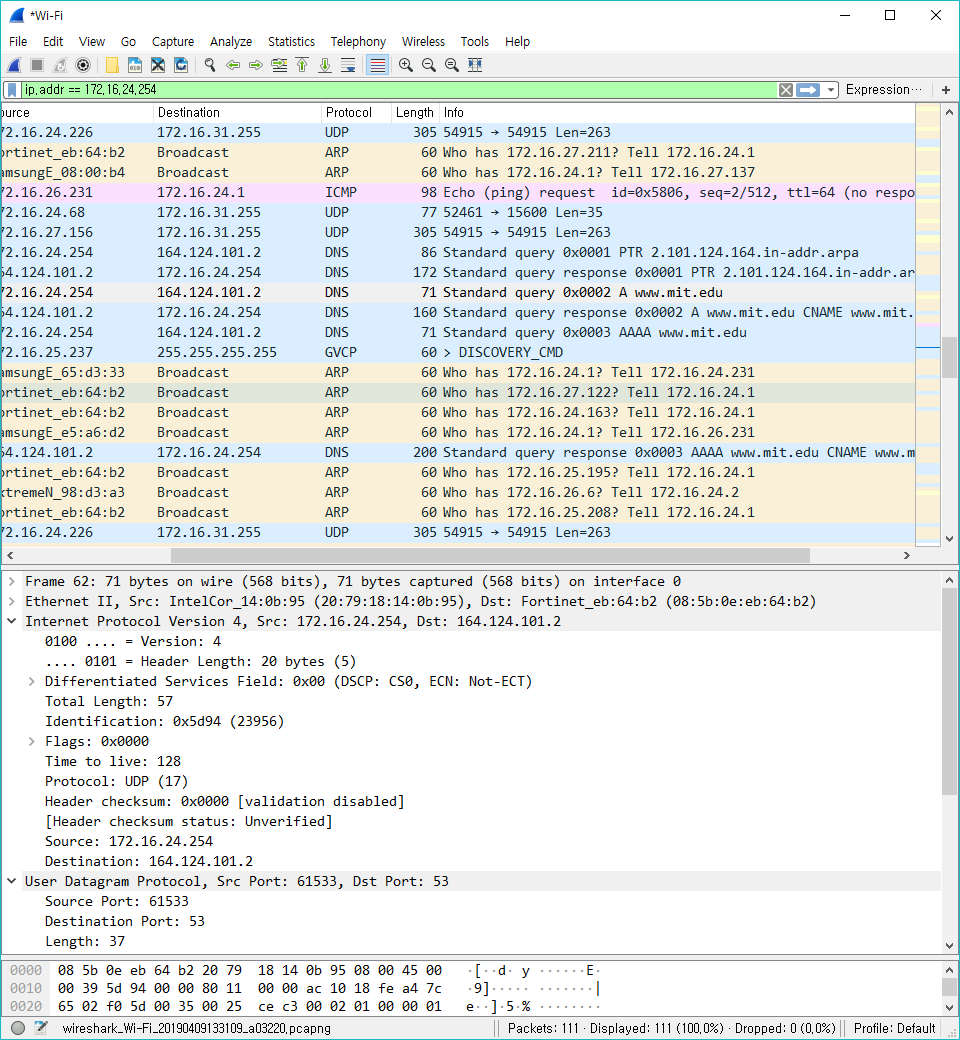


10.이 웹페이지에는 이미지가 있습니다. 각 이미지를 검색하기 전, 호스트가 새 DNS 쿼리를 발행합니까?

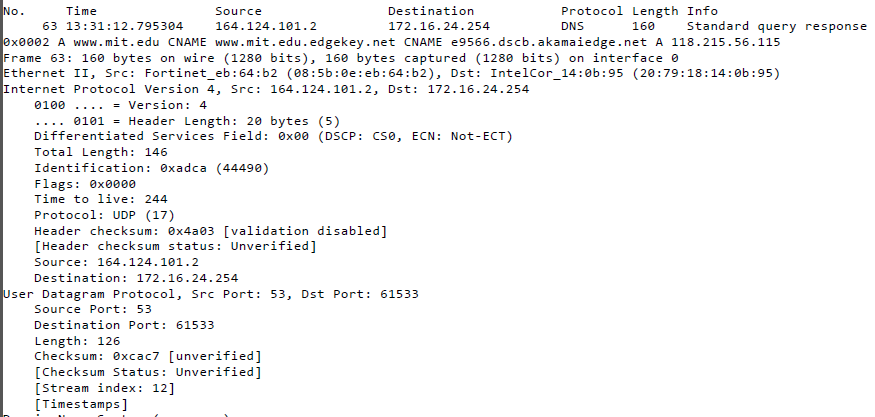


새로운 DNS를 발행하지 않습니다.

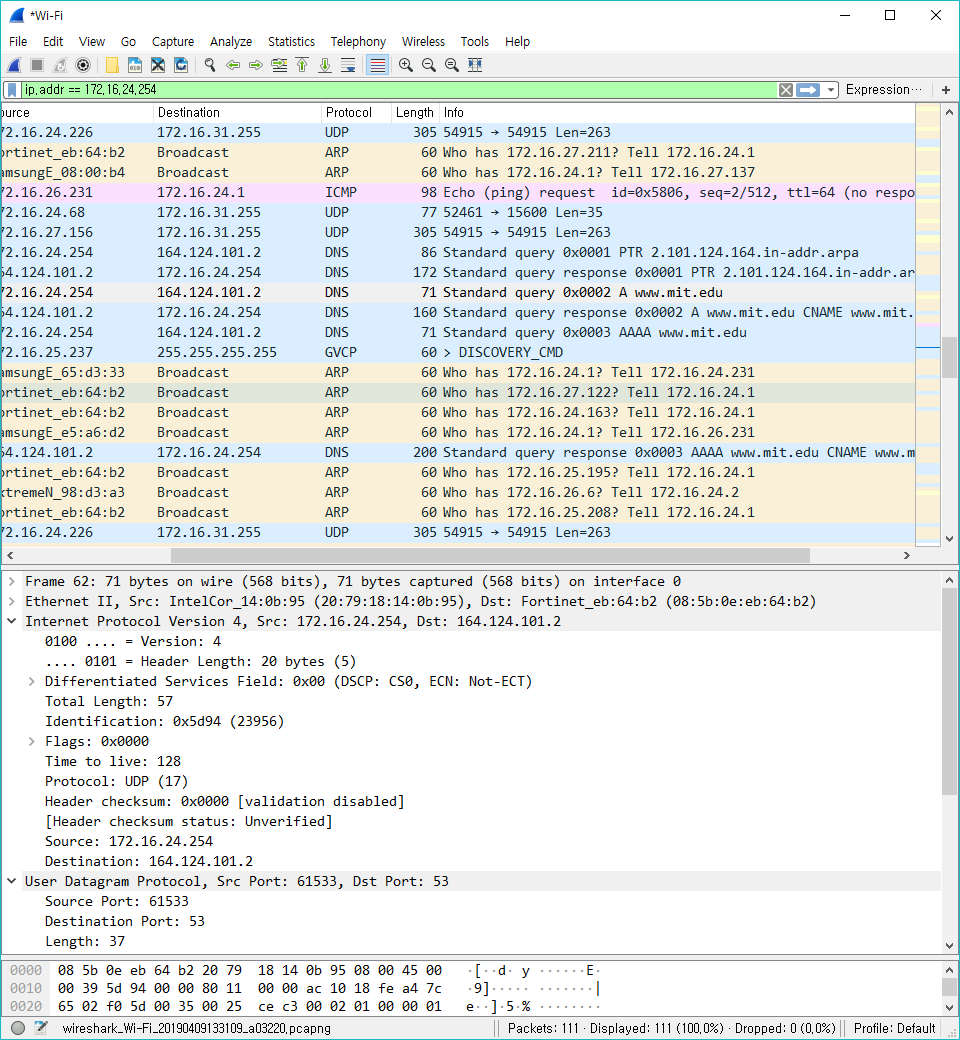
11. DNS 쿼리 메시지의 대상 포트는 무엇입니까? DNS 응답 메시지의 소스 포트는 무엇입니까?



쿼리 메시지의 대상 포트 : 53

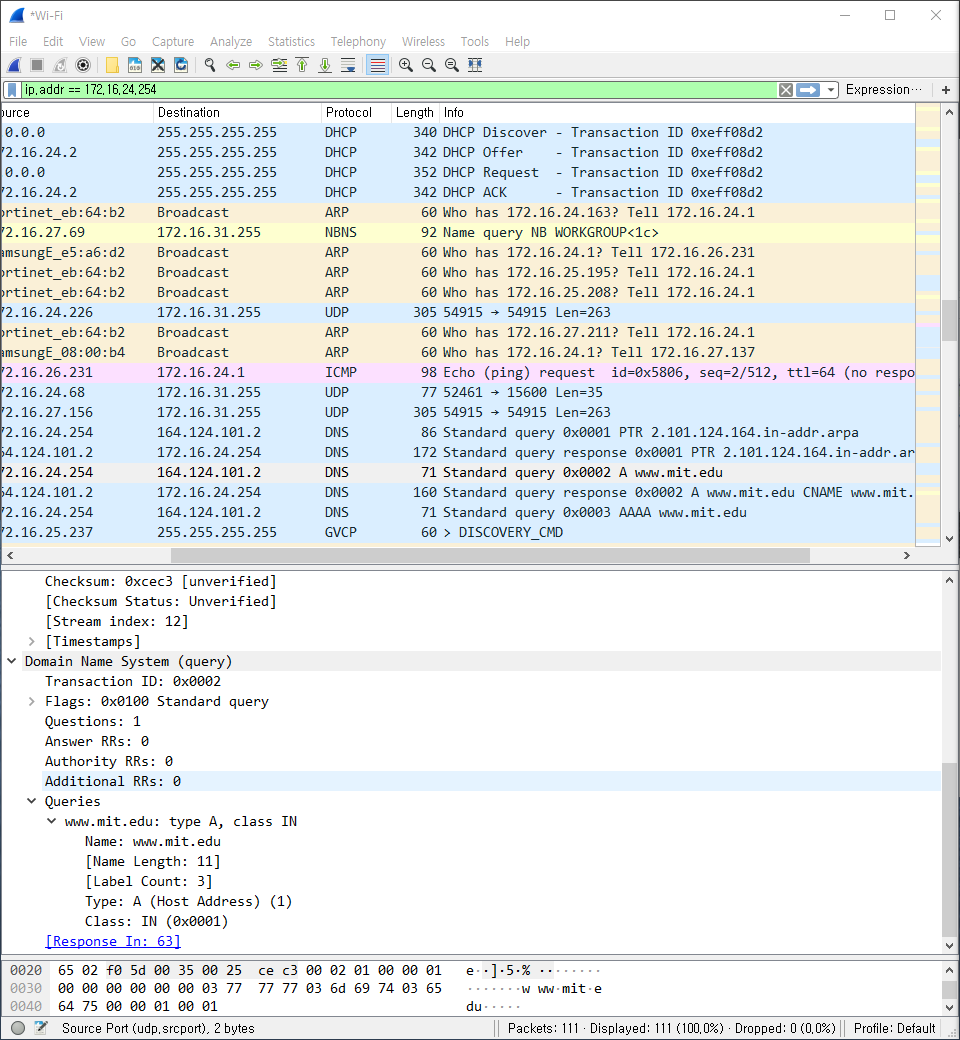


응답메시지의 소스포트 : 53

12. DNS 쿼리 메시지는 어떤 IP 주소로 전송됩니까? 해당 주소는 기본 로컬 DNS 서버의 IP 주소입니까? 

쿼리 메시지의 전송 주소 : 164.124.101.2

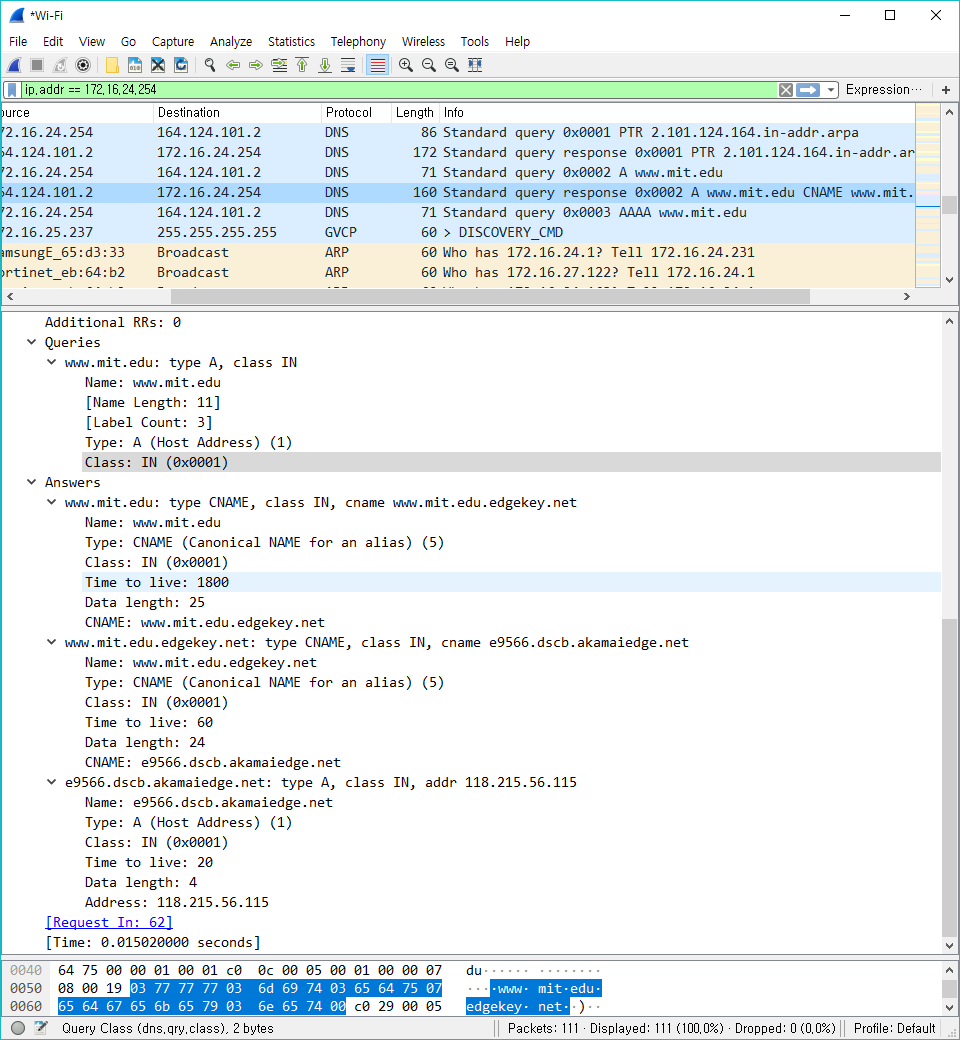
네 동일합니다. 6번에 참조된 DNS 서버 참조

13. DNS 쿼리 메시지를 확인하십시오. DNS 쿼리의 “타입”은 무엇입니까? 쿼리 메시지에 “답변”이 포함되어 있습니까? 

DNS 쿼리의 타입 : A

답변은 포함되어 있지 않습니다.

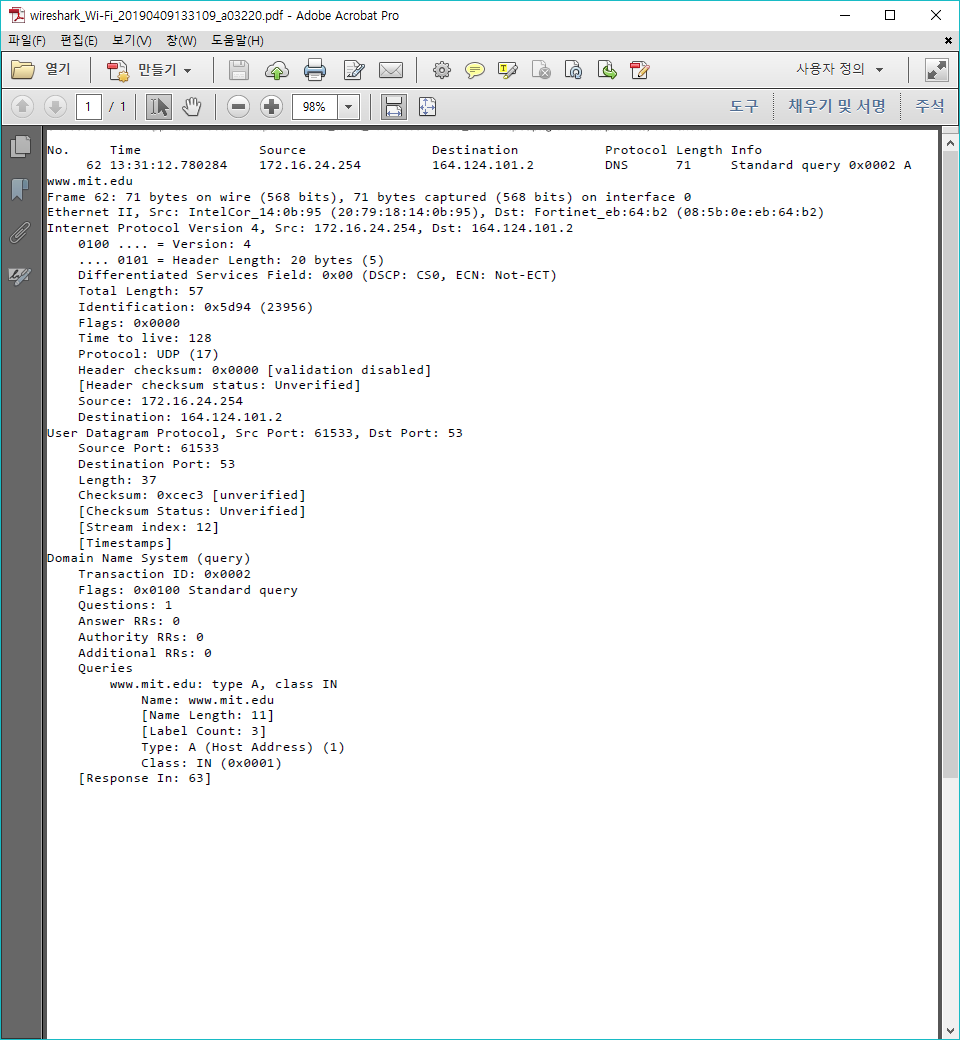
14. DNS 응답 메시지를 확인하십시오. 응답 메시지가 제공하는 MIT 네임서버는 무엇입니까? 해당 응답 메시지가 MIT 네임서버의 IP 주소도 제공합니까?

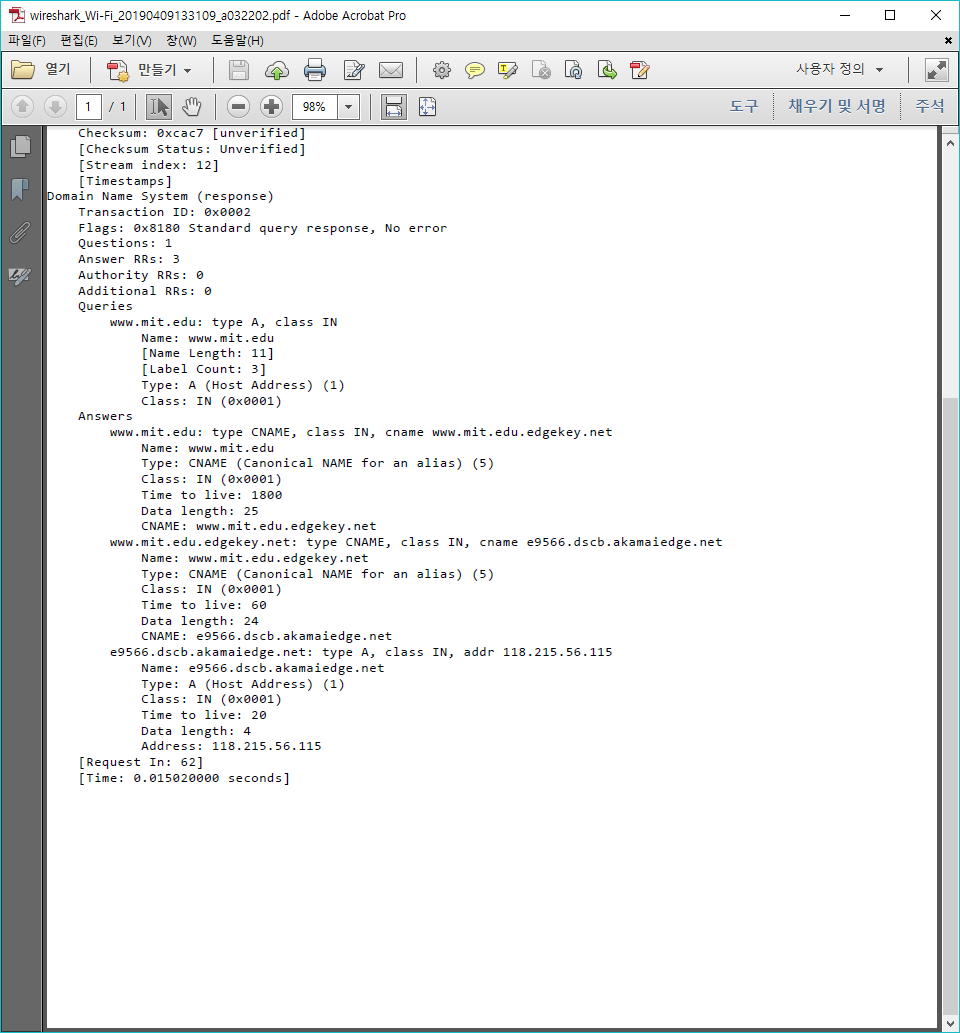
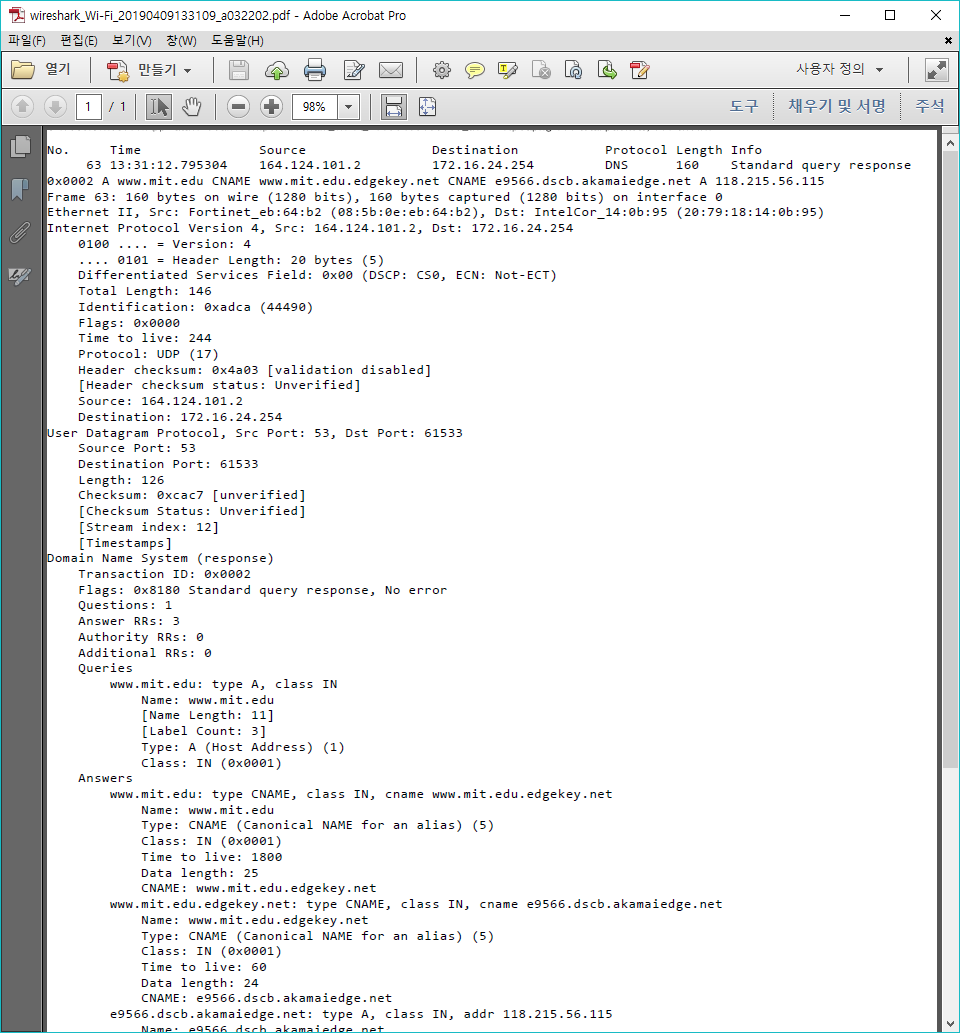


MIT 네임서버 : e9566.dscb.akamaiedge.net

IP주소도 제공하며 해당 IP 주소는 118.215.56.115입니다.

15. 전체 결과를 스크린샷을 첨부하십시오





다음을 물음에 답을 하세요.

16. DNS 쿼리 메시지는 어떤 IP 주소로 전송됩니까? 해당 주소는 기본 로컬 DNS 서버의 IP 주소입니까?

164.124.101.2의 주소로 전송됩니다.

네, 해당 주소는 기본 로컬 DNS 서버의 IP주소입니다.

(16번부터는 화면 캡쳐를 사용하지 않은 관계로 Wireshark Print 기능을 사용한 PDF파일을

캡쳐하여 첨부하였습니다. 19번을 참조해주시기 바랍니다.)

17. DNS 쿼리 메시지를 확인하십시오. DNS 쿼리의 “타입”은 무엇입니까? 쿼리 메시지에 “답변”이 포함되어 있습니까?

DNS 쿼리의 타입 : NS

해당 메시지에 답변이 포함되어 있지 않습니다.

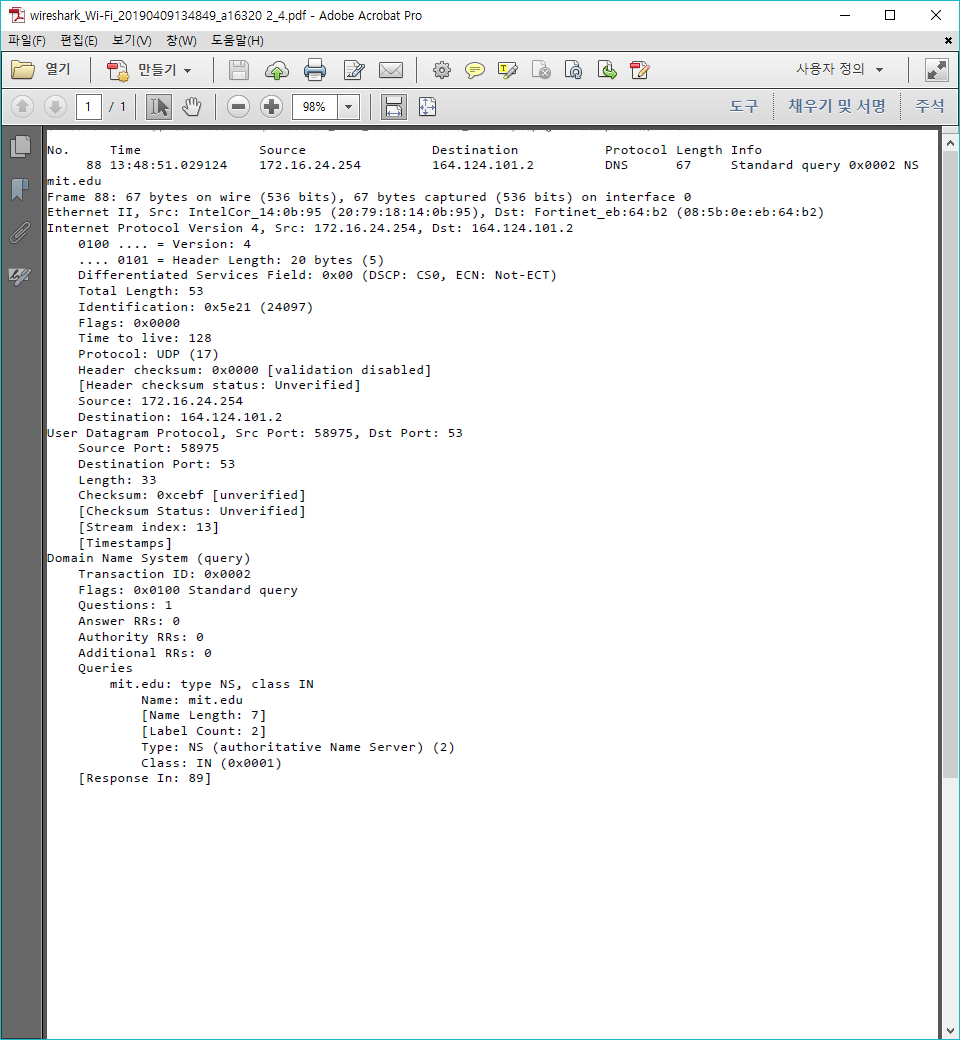
18. DNS 응답 메시지를 확인하십시오. 응답 메시지가 제공하는 MIT 네임서버는 무엇입니까? 해당 응답 메시지가 MIT 네임서버의 IP 주소도 제공합니까?

응답 메시지가 제공하는 MIT 네임 서버는 총 8개로

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

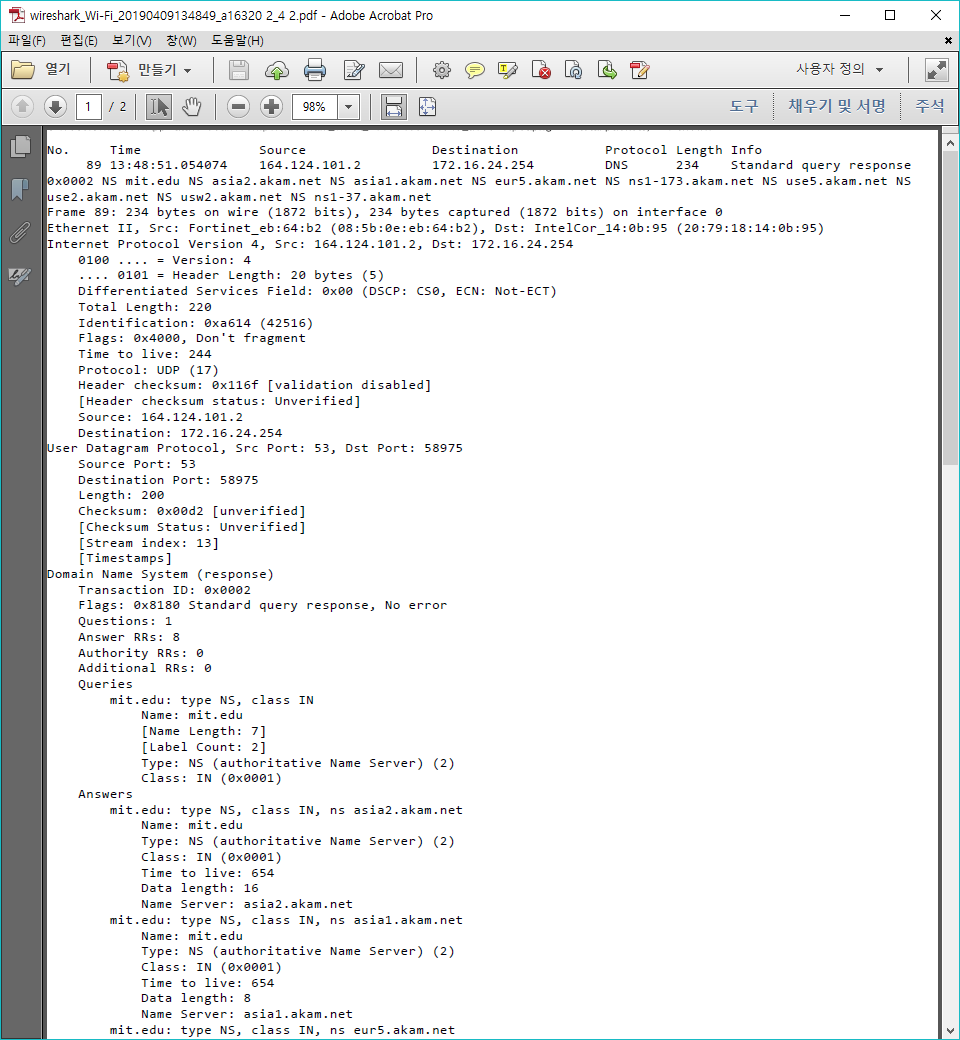
이며 IP주소는 제공되지 않습니다.

19. 전체 결과를 스크린샷을 첨부하십시오



문제 17.

문제 16.



문제 18.

