

# IT CookBook, 쉽게 배우는 데이터 통신과 컴퓨터 네트워크(개정) 14장 연습문제 해답

본 자료의 저작권은 박기현과 한빛아카데미에 있습니다.

이 자료는 강의 보조자료로 제공되는 것으로, 학생들에게 배포되어서는 안 됩니다.

1. ① IP 주소, ② 도메인 이름, ③ DNS
2. ① 0, ② 10, ③ 110, ④ 멀티캐스팅
3. ① 해석기(Resolver), ② UDP, ③ DNS 네임 서버
4. ① 도메인 네임 스페이스, ② 네임 서버, ③ 해석기
5. ① 존
6. ① 해석기, ② 네임 서버
7. ① 인증 데이터, ② 캐시 데이터
8. ① UDP, ② 512, ③ TCP

9. ①, ②, ③, ④

(설명⑤) nslookup은 주소 변환 기능을 제공하는 사용자 명령으로, 주어진 도메인 이름에 해당하는 IP 주소를 찾아 주며, 반대의 변환 기능도 수행한다.

10. ①, ②, ③

(설명④) 해석기는 네임 서버로부터 클라이언트의 요청 정보를 얻어내는 프로그램이다.

(설명⑤) 해석기는 처음 접촉한 네임 서버로부터 도메인 정보가 없으면 다른 네임 서버에 접촉해 질의를 계속 이어간다.

11. ②

(설명②) 도메인 이름은 최하위에 위치한 호스트의 레이블을 맨 왼쪽에 적고, 상위 노드로 이동하면서 점으로 구분한 레이블 이름을 연속으로 붙인다.

12. 없음

13. ①, ②, ④, ⑤

(설명③) 질의 레코드는 DNS 클라이언트가 DNS 서버에 정보를 요청하는 용도로

사용되며, 세 개의 필드로만 구성된다.

14. ①

(설명①) 도메인 이름과 호스트 주소 변환 정보를 원하는 응용 프로그램은 해석기라고 불리는 DNS 클라이언트에게 정보 제공을 요청한다.

15. ①, ②, ③, ⑤

(설명④) 해석기와 네임 서버는 53번 포트를 기본으로 사용하여 UDP로 DNS 메시지를 전송한다.

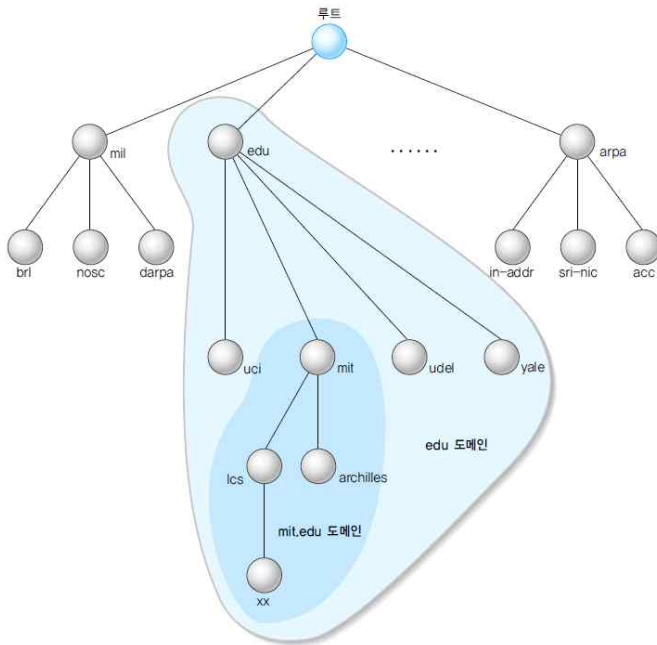
16.

인터넷 사용자가 호스트를 지칭할 때 사용하는 일반 주소 표현 방법은 문자형으로 표기하는 도메인 이름(Domain Name)이다. 도메인 이름을 네트워크에서 사용하려면 도메인 이름과 IP 주소 사이의 변환 과정이 필요하다.

인터넷 보급이 미미하던 시절에는 특정 컴퓨터 시스템이 전체 호스트의 명칭을 관리하도록 지정되어, 도메인 이름과 IP 주소의 매핑 정보를 관리하였다. 즉, 이 시스템의 특정 파일에 모든 호스트의 명칭 정보를 도메인 이름과 IP 주소의 쌍으로 관리하였다. 그리고 특정 파일을 다른 모든 컴퓨터가 복사함으로써 호스트 주소 정보의 일관성을 유지하였다. 컴퓨터 보급이 늘면서 이런 업무를 수작업으로 관리하기 어려워지기 시작하였다. 특히 호스트 수가 엄청나게 증가하면서 한 시스템에서 모든 호스트의 이름을 유지하기가 현실적으로 불가능해졌다. 또한 도메인 이름을 중복 사용하지 않도록 통제하기 쉽지 않았다. 이런 문제점을 해결하려고 고안된 것이 DNS 서비스다.

17.

도메인이라는 명칭은 도메인 네임 스페이스에 있는 하부 트리 전체를 의미하며, 해당 도메인의 이름은 하부 트리의 맨 상위에 위치한 호스트의 도메인 이름이다. 예를 들어, [그림 15-2]는 바깥 부분의 edu 도메인과 안쪽 부분의 mit.edu 도메인을 설명한다.



[그림 15-2] 도메인 네임 스페이스(RFC 1034 참고)

18.

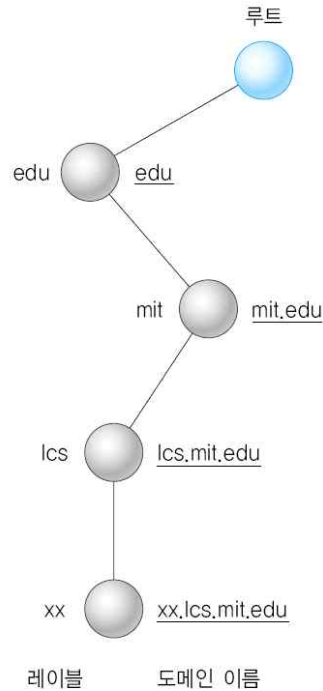
TLD(Top Level Domain, 최상위 도메인)은 RFC 1591에서 세 글자로 구성된 최상위 도메인 7개를 정의하고 있다. 최초의 최상위 도메인 레이블은 다음과 같다.

- com : 상업적인(Commercial) 용도로 사용하며, 이용자의 규모가 매우 방대하다.
- edu : 교육기관(Educational Institutions)을 위해 정의되었으나, 나중에 4년제 대학 기관으로 한정되었다.
- net : 네트워크(Network) 서비스 제공자와 관련된 시스템을 위해 정의되었다.
- org : 다른 TLD에 속하지 않는 비정부 기구를 포함한다. 다양한 종류의 기관(Organization)을 위해 정의되었다.
- int : 국제적인 목적으로 정의되었으나, 현재는 새로운 사용자의 등록이 유보되어 있다.
- gov : 미국의 주 정부를 비롯해 미국 연방 정부와 관련된 기관을 위해 정의되었으나, 현재는 연방 정부와 관련된 기관에서만 사용한다.
- mil : 미국 국방성 관련 기관에서 사용하도록 정의되었다.

인터넷 사용자의 증가로 7개 도메인으로 모든 수요를 충족시킬 수 없게 됨에 따라 최근 에 arts, firm, info, nom, rcc, store, web 같은 도메인이 추가로 정의되었다.

[그림 15-3]처럼 레이블이 부여된 각 호스트는 도메인 이름(Domain Name)을 갖는다. 도메인 이름은 하위 호스트의 레이블부터 시작해 루트 호스트까지의 경로에 위치한 모든

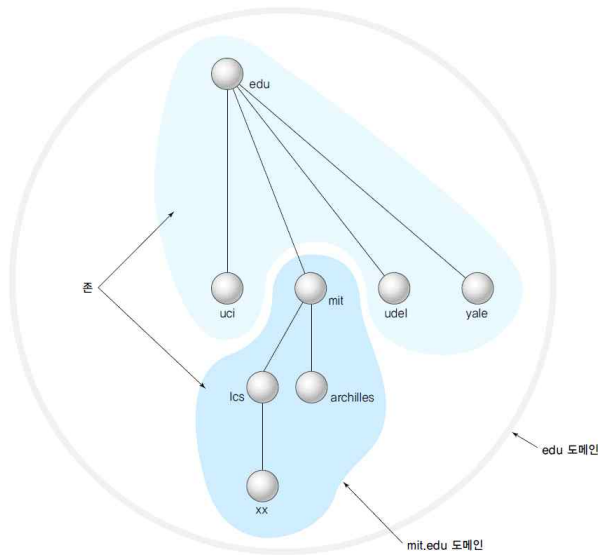
호스트의 레이블 이름에 점(.)을 붙여 연결한다. 예를 들어, lcs 레이블이 붙은 호스트는 lcs와 루트쪽 경로에 위치한 mit, edu 레이블을 사용해 lcs.mit.edu라는 도메인 이름을 갖는다.



[그림 15-3] 도메인 이름과 레이블

19.

도메인이 인터넷 주소의 지정 단위라면, 존(Zone)은 임의의 네임 서버가 관리하는 영역이다. 도메인과 존은 의미가 유사하면서도 약간 다르다. 특정 네임 서버가 자신의 하위에 위치한 도메인을 전적으로 관리하면 존과 도메인이 동일하지만, 하부에 새로운 도메인이 추가되면 두 영역이 일치하지 않는다. 예를 들어 [그림 15-5]를 살펴보자. edu 도메인의 하부에 mit.edu라는 도메인이 존재하므로 edu 도메인에는 edu와 mit.edu 네임 서버가 모두 동작한다. 따라서 edu 도메인에는 서로 구분되는 존이 두 개 존재한다. mit.edu 아래에 위치한 노드의 정보는 mit.edu 네임 서버가 전적으로 관리한다.

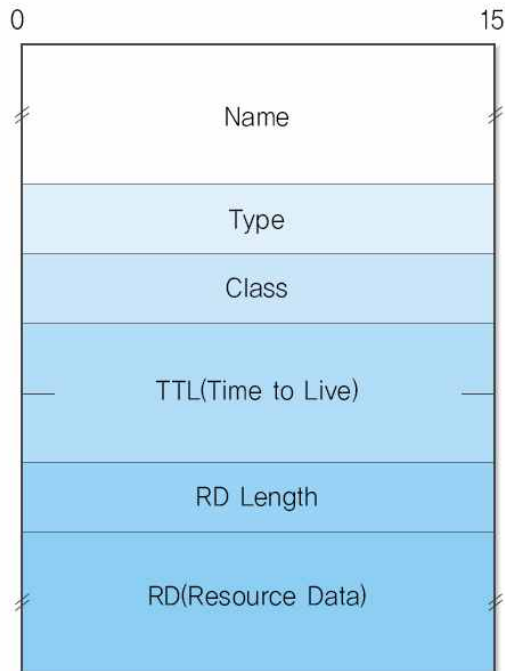


[그림 15-5] 도메인과 존

20.

#### ■ 자원 레코드

DNS 서비스는 이름과 주소 정보를 저장하기 위한 데이터베이스므로 레코드 개념이 필요하다. 자원 레코드(RR, Resource Record)라는 개념을 사용해 DNS 데이터를 저장한다. 트리에 연결된 각 호스트는 자원 레코드와 관계되며, 네임 서버의 데이터베이스는 자원 레코드로 구성된다. 따라서 DNS 네임 서버가 DNS 클라이언트인 해석기에 반환하는 데이터는 자원 레코드가 된다. 자원 레코드의 구조는 다음 그림과 같다.



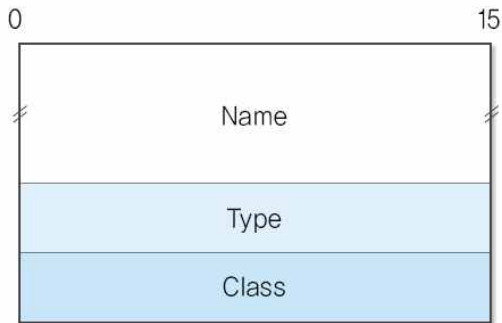
자원 레코드

자원 레코드를 구성하는 필드의 의미는 다음과 같다.

- Name(이름) : 찾고자 하는 가변 길이의 도메인 이름이다. 질의 레코드에 기록되어 DNS 서버에 요청된다.
- Type(유형) : 16비트 크기로 자원의 종류를 나타낸다.
- Class(클래스) : 프로토콜 패밀리를 의미하는데, 인터넷에서는 IN 값을 사용한다.
- TTL(Time To Live, 생존 기간) : 자원 레코드가 만기될 때까지의 유효 시간을 초 단위로 표시한다. 특정 호스트에 캐시된 정보가 만기되어 버려질 때까지 얼마나 오래 저장되어 사용할 수 있는지를 나타낸다.
- RD Length(RD 길이) : 자원 데이터의 길이를 바이트 단위로 나타낸다.
- RD(자원 데이터) : 자원 레코드와 관계된 데이터가 기록되는데, 자원 레코드의 유형 값에 따라 내용의 구성과 크기가 달라진다.

#### ■ 질의 레코드

질의 레코드(Query Record)는 DNS 클라이언트가 DNS 서버에 정보를 요청하는 용도로 사용되며, [그림 15-6]처럼 Name, Type, Class라는 세 개의 필드로 구성된다. 질의 레코드와 자원 레코드는 DNS 메시지에서 구분되어 사용된다. 질의 레코드는 다음 그림과 같다.



질의 레코드

다음은 주요 자원 레코드 유형이다.

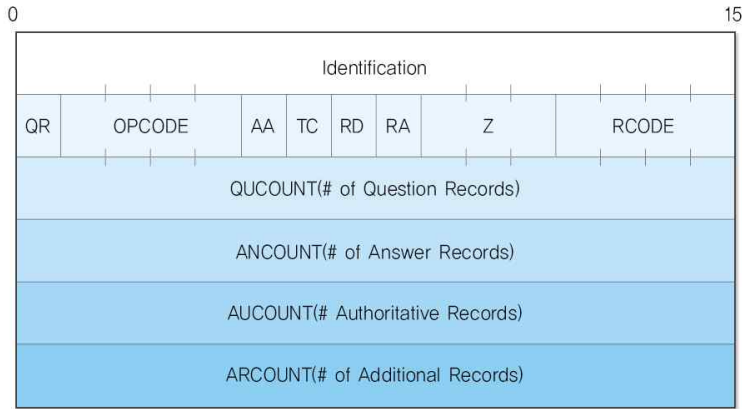
- Name(이름) : 찾고자 하는 가변 길이의 도메인 이름이다. 질의 레코드에 기록되어 DNS 서버에 요청된다.
- Class(클래스) : 프로토콜 패밀리를 의미하는데, 인터넷에서는 IN 값을 사용한다.
- Type : 도메인 네임 서버는 관리하는 모든 정보를 자원 레코드에 저장하며, 서로 다른 목적을 달성하기 위해 다수의 자원 레코드 유형을 정의한다.
  - A(Address) : 호스트의 IP 주소를 의미하며 도메인 이름을 IP 주소로 변환하는데 사용된다.
  - NS(Name Server) : 도메인을 관장하는 인증된 네임 서버를 나타낸다.
  - CNAME(Canonical Name) : 자원에 대한 접근을 단순화하려고 사용되며, 호스트 이름의 별명을 지원한다.
  - SOA(Start of Authority) : 존의 시작을 표시한다.
  - WKS(Well-known Services) : 호스트가 제공하는 네트워크 서비스를 정의한다.
  - PTR(Pointer) : IP 주소를 도메인 이름으로 변환하는 데 사용한다.
  - HINFO(Host Information) : 호스트 정보를 의미하며, 호스트가 사용하는 하드웨어와 운영체제에 관한 정보를 제공한다.

21.

인증 데이터(Authoritative Data)는 해당 데이터를 직접 관리할 책임이 있는 네임 서버로부터 받은 정보를 의미한다. 반면, 캐시 데이터(Cached Data)는 이전 요청에 의해 호스트가 보관하던 데이터며, 재사용할 목적으로 한동안 저장한다. 일반적으로 인증 데이터는 현재의 네트워크 상태를 그대로 반영한 정확한 데이터지만, 인터넷의 안정도를 감안할 때 캐시 데이터를 사용해도 크게 문제되지는 않는다.

22.

DNS 메시지의 헤더 구조는 다음과 같다.



DNS 메시지 헤더

Identification 필드는 클라이언트의 질의에 대해 회신된 응답이 서로 연관되는지 확인한다. 즉, 클라이언트는 질의 요청을 보낼 때마다 서로 다른 번호를 부여하고, 서버는 해당하는 응답 메시지에 이 번호를 복사해서 회신한다.

플래그 필드에는 비트 정보가 8개 존재하는데, 각각은 다음과 같은 기능을 수행한다.

- QR(Query Response) : 메시지 종류를 나타낸다. 0이면 질의 메시지고, 1이면 응답 메시지다.
- OPCODE : 질의나 응답 종류를 나타낸다. 0은 표준, 1은 인버스, 2는 서버 상태 요청이다.
- AA(Authoritative Answer) : 네임 서버가 인증 권한이 있는 서버임을 나타내므로 응답 메시지에만 사용된다.
- TC(Truncated) : 1로 지정하면 응답의 크기가 UDP의 최대 크기인 512바이트를 초과하여 512바이트 크기로 잘렸음을 알려준다. 초과되어 잘린 데이터를 처리하는 후속 동작이 이루어져야 한다.
- RD(Recursion Desired) : 1이면 재귀적인 응답을 원함을 뜻한다. 질의 메시지에서 사용된다.
- RA(Recursion Available) : 응답 메시지에서 사용되며, 반복 응답이 가능하다는 의미다.
- Z : 예약 필드로 000으로 지정된다.
- RCODE : 응답 메시지에서 응답 오류를 나타내는 데 사용되며, 0이면 오류가 없다는 의미다.

QUCOUNT는 DNS 메시지의 Question 필드에 있는 질의 요청의 개수를 의미하고, ANCOUNT는 응답용 DNS 메시지에서 답변 레코드의 개수다. AUCOUNT는 응답용 DNS 메시지에서 인증 레코드의 개수, ARCOUNT는 부가 정보 레코드의 개수다.

23.

DNS 메시지가 512바이트보다 작으면 UDP를 사용하는 데 문제가 없지만, 이보다 크면 TCP를 사용해야 한다. TCP를 사용할 때는 다음 두 가지 경우를 고려할 수 있다. 첫째, 응



답 메시지가 512바이트보다 크다는 사실을 해석기가 미리 인지하는 경우로, 이때는 처음부터 TCP 연결을 사용한다. 둘째, 해석기가 사전에 인지하지 못한 상태에서 UDP를 사용하는 경우다. 이럴 때는 응답 메시지의 헤더에 있는 TC 플래그가 1로 지정되므로, 해석기가 TCP 연결을 설정하여 올바른 응답을 요청할 수 있다.

24.

가장 간단한 예로 해석기가 [www.korea.co.kr](http://www.korea.co.kr)라는 호스트의 IP 주소를 찾으려고 로컬 네임 서버에 질의 메시지(Query Message)를 전송하는 경우를 가정해보자.

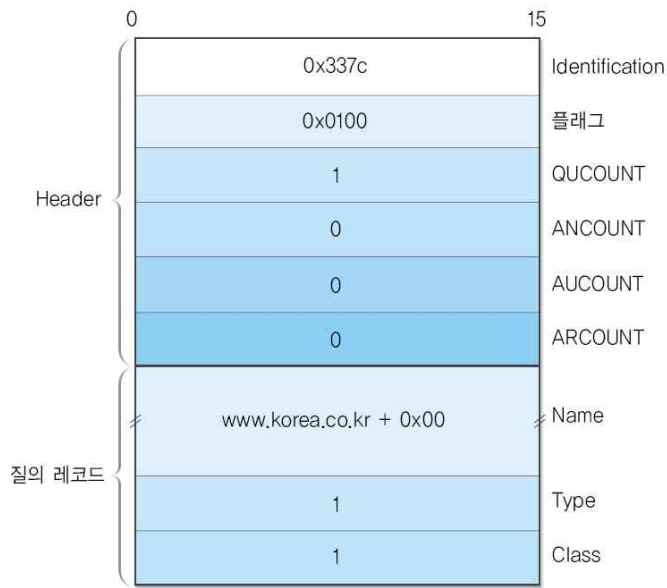
DNS 메시지([그림 15-9] 참조)는 DNS 메시지 헤더 메시지([그림 15-10] 참조)부터 시작된다. 헤더의 첫 번째에 위치한 Identification은 메시지 식별자로, UDP의 비순서적 전송 방식을 보완하려고 사용된다. 해석기는 이 번호를 사용해 서버의 응답을 순서대로 정렬하여 질의와 응답이 적절히 연결되도록 해준다. 플래그 값은 0x0100이므로 QR=0은 질의 메시지, OPCODE=0은 표준 질의, RD=1은 재귀적 응답임을 나타낸다.

```
Identification: 0x337c
플래그: 0x0100 (QR=0, Opcode=0000, AA=0, TC=0, RD=1, RA=0, Z=000,
RCODE=0000)
QUCOUNT: 1
ANCOUNT: 0
AUCOUNT: 0
ARCOUNT: 0
```

QUCOUNT 값만 1이므로 [그림 15-9]에서 헤더에 이어지는 필드는 질문에 관한 질의 레코드 하나임을 알 수 있다. [그림 15-6(b)]에 나타난 질의 레코드 값은 다음과 같으며, 이는 찾는 정보가 [www.korea.co.kr](http://www.korea.co.kr) 호스트의 IP 주소임을 의미한다.

```
Name: www.korea.co.kr
Type: A (Address)
Class: IN (인터넷)
```

위 값을 DNS 메시지로 형식화하면 [그림 15-11]과 같다. Header에는 앞서 소개한 이진 값이 기록되고, 질의 레코드의 도메인 이름에는 [www.korea.co.kr](http://www.korea.co.kr)이 기록되는데, 이름 끝에는 0x00을 추가하여 이름의 마지막임을 표시해야 한다. 도메인 유형 A는 값이 1이며, 도메인 클래스 IN도 값이 1이다.



[그림 15-11] 질의 메시지의 예

25.

(연습문제 8번)의 [그림 15-11]과 같은 질의 메시지를 수신한 네임 서버는 DNS 클라이언트가 원하는 IP 주소를 찾아 응답 메시지(Response Message)로 회신해야 한다. Identification은 클라이언트의 값을 그대로 사용해야 하며, 플래그는 0x8180 값으로 주어졌다. 이 값을 해석하면 QR=1 이므로 응답 메시지가 되고, OPCODE는 여전히 표준 질의 응답임을 나타낸다. RD=1, RA=1이므로 재귀적 질의응답임을 알 수 있으며, RCODE 정보에 의해 오류는 발생하지 않았다.

```

Identification: 0x337c
플래그: 0x08180 (QR=1, Opcode=0000, AA=0, TC=0, RD=1, RA=1, Z=000,
RCODE=0000)
QUCOUNT: 1
ANCOUNT: 2
AUCOUNT: 2
ARCOUNT: 0
  
```

해석기의 요청을 받는 서버는 도메인의 인증 권한을 갖지 않은 것으로 가정되어 메시지에 재귀적 응답이 포함되어 있다. 따라서 Question 자원 레코드 하나, Answer 자원 레코드 두 개, 인증 권한을 가진 네임 서버를 가리키는 Authority 자원 레코드가 두 개 있다. 그리고 부가 정보에 관한 자원 레코드는 회신되지 않았다. Question 레코드는 다음과 같

이 질의 메시지의 경우와 같다.

```
Name: www.korea.co.kr
Type: A (Address)
Class: IN (인터넷)
```

응답 메시지에는 자원 레코드가 두 개 존재하는데, 첫 번째의 유형이 CNAME으로 되어 있다. 이를 통해 www.korea.co.kr는 호스트의 정식(Canonical) 명칭이 아니고 별명(Alias)에 해당함을 알 수 있다. 자원 데이터를 통해 정식 명칭은 korea.co.kr이고, 원하는 IP 주소는 211.223.201.30임을 알 수 있다.

```
Name: www.korea.co.kr
Type: CNAME (Canonical Name for an Alias)
Class: IN (인터넷)
TTL: 2시간
RD Length: 2
RD: Primary name: korea.co.kr
Name: korea.co.kr
Type: A (Address)
Class: IN (인터넷)
TTL: 2시간
RD Length: 4
RD: Addr: 211.223.201.30
```

TTL 값은 제공된 정보가 캐시 상태로 유지될 수 있는 최대 시간을 의미하며, RD Length는 자원 데이터의 크기를 바이트로 나타낸다. 예를 들어 IP 주소의 크기는 4바이트다. 자원 데이터는 자원 레코드 유형에 따라 값이 달라진다. NS 유형은 인증 네임 서버의 도메인 이름을 보관하고, CNAME 유형은 정식 명칭, A 유형은 IP 주소를 나타낸다. 다음은 인증 자원 레코드의 내용이다.

Name: korea.co.kr  
Type: NS (Authoritative Name Server)  
Class: IN (인터넷)  
TTL: 2시간  
RD Length: 8  
RD: Name Server: ns.ns1.kr  
Name: korea.co.kr  
Type: NS (Authoritative Name Server)  
Class: IN (인터넷)  
TTL: 2시간  
RD Length: 10  
RD: Name Server: nsbk.ns2.kr