[AI.SW개론-F]

Wireshark를 활용한 기능 중심적 DNS 분석

네트워크 프로토콜 분석 보고서: DNS(Domain Name System) 분석

202578218 정지은 AISW계열

목차

Ⅰ. **DNS(Domain Name System)**의 개요

DNS(Domain Name System)은 인터넷의 전화번호부로써 사람들은 도메인 이름을 통해 온라인에서 정보를 접근할 수 있다. 웹 브라우저는 인터넷 프로토콜(IP) 주소를 통해 상호작용하고, 이 DNS가 도메인 이름을 IP 주소로 변환하여 브라우저가 인터넷 리소스를 불러올 수 있도록 한다. 인터넷에 연결된 각 장치는 고유한 IP 주소를 가지며, 다른 장비들은 이 주소를 통해 해당 장치를 찾는다.

DNS는 인터넷을 위한 디렉터리 조회 기능을 제공함으로써, 사람들에게 인터넷 탐색을 더 쉽게 만들어주며, 온라인 서비스가 매우 탄력적으로 유지되도록 돕는다. 즉, DNS는 하나의 서버가 아닌 여러 개의 서버를 통해 서비스를 제공한다.

DNS는 1983년 표준화된 이후로 많은 개선과 확장이 이루어졌지만, 프라이버시 측면에서는 거의 발전이 없었다. DNS 정보는 암호화되지 않은 채 인터넷을 통해 전송되며, 이는 해당 경로에 있는 누구나 볼 수 있다는 뜻이다. 따라서 최근에는 암호화의 중요성이 강하게 대두되고 있다.

Ⅱ. 웹페이지를 불러오기 위해 필요한 **DNS** 서버 **4**가지

DNS 리커서 **(recursor)**

리커서는 도서관에서 특정 책을 찾아달라고 요청받은 사서처럼 생각할 수 있다. DNS 리커서는 웹 브라우저 같은 클라이언트 애플리케이션으로부터 질의를 수신하기 위해 설계된 서버이다. 일반적으로 리커서는 클라이언트의 DNS 질의를 만족시키기 위해 추가 요청을 수행할 책임이 있다.

루트 네임서버 **(root nameserver)**

루트 서버는 사람이 읽을 수 있는 호스트 이름을 IP 주소로 번역하는 첫 번째 단계이다. 도서관의 인덱스처럼 생각할 수 있으며, 보다 구체적인 위치들을 가리키는 참고 자료 역할을 한다.

TLD 네임서버 **(Top Level Domain nameserver)**

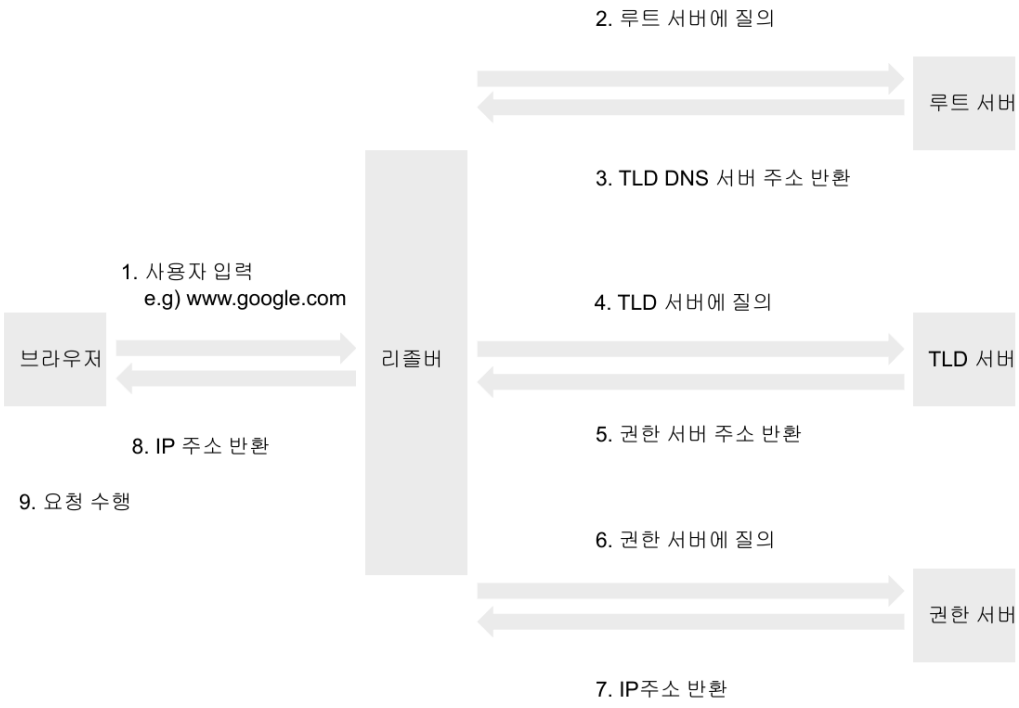
TLD 서버는 도서관의 특정 책장처럼 생각할 수 있다.이 서버는 특정 IP 주소를 찾기 위한 다음 단계이며, 호스트 이름의 마지막 부분을 관리한다 (example.com에서는 "com").

권한 있는 네임서버 **(authoritative nameserver)**

이 마지막 네임서버는 책장 위의 사전처럼 생각할 수 있다. 특정 이름을 정의로 번역할 수 있는 사전이다. 이 네임서버는 질의 체인의 마지막 지점으로, 요청된 레코드에 접근할 수 있다면 해당 호스트 이름의 IP 주소를 DNS 리커서에게 반환한다.

Ⅲ. DNS 동작 8단계

웹 브라우저는 사람들이 사람 친화적인 도메인 이름을 사용할 수 있게 하지만, 브라우저는 IP 주소를 사용하여 필요한 리소스를 식별하고 연결한다. 이 작업을 위해 브라우저는 DNS를 통해 도메인 이름을 정확한 IP 주소로 변환하며, 이 과정은 사용자에게는 보이지 않는다.



사용자가 브라우저에 example.com을 입력하고, 인터넷을 통해 DNS 재귀 리졸버로 전달된다. 리졸버는 루트 네임서버에게 질의하고, 루트 서버는 .com 같은 TLD DNS 서버 주소를 리졸버에 반환한다. 이 다음 리졸버는 .com TLD 서버에 질의하고, TLD 서버는 example.com의 권한 네임서버 주소를 반환한다. 리졸버는 example.com 권한 네임서버에 질의하고, 권한 서버는 example.com의 IP 주소를 리졸버에게 반환한다. 리졸버는 이 IP 주소를 웹 브라우저에게 반환하여 브라우저는 웹페이지 요청을 수행한다. 이후 브라우저는 해당 IP 주소에 HTTP 요청을 보내고, 웹 서버는 페이지를 반환하여 브라우저에 표시된다.

Ⅳ. 메시지 구조

DNS(Domain Name System) 메시지는 질의(query) 메시지와 응답(answer) 메시지를 포함하며, 이 구조는 헤더 부분과 내용 부분으로 나뉘고 헤더는 메시지의 유형, 질의 또는 응답

여부, 메시지의 길이 등을 나타내고, 내용 부분에는 질의 또는 응답에 대한 세부 정보가 포함된다.

헤더 부분

-ID (Identifier): 질의 또는 응답 메시지를 식별하기 위한 16비트의 고유한 식별자이다.

-Flags: 메시지의 유형 (질의 또는 응답), 재귀적인 질의 여부, 오류 여부 등을 나타내는 16비트의 플래그이다.

-QDCOUNT (Question Count): 질의 부분에 포함된 질의 레코드의 수를 나타낸다.

-ANCOUNT (Answer Count): 응답 부분에 포함된 응답 레코드의 수를 나타낸다.

-NSCOUNT (Name Server Count): 이름 서버 레코드의 수를 나타낸다.

-ARCOUNT (Additional Records Count): 추가 레코드의 수를 나타낸다.

내용 부분

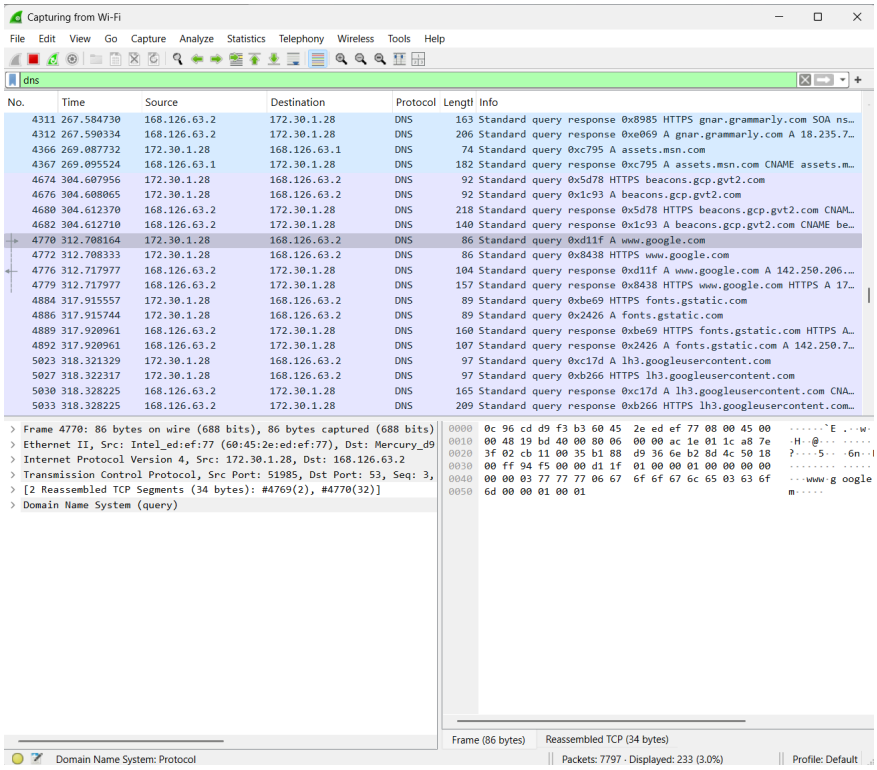
-질의 부분 (Question Section): 질의하는 도메인 이름, 질의 유형 (예: A 레코드, MX 레코드 등), 질의 클래스 (예: IN, CHR) 등이 포함된다.

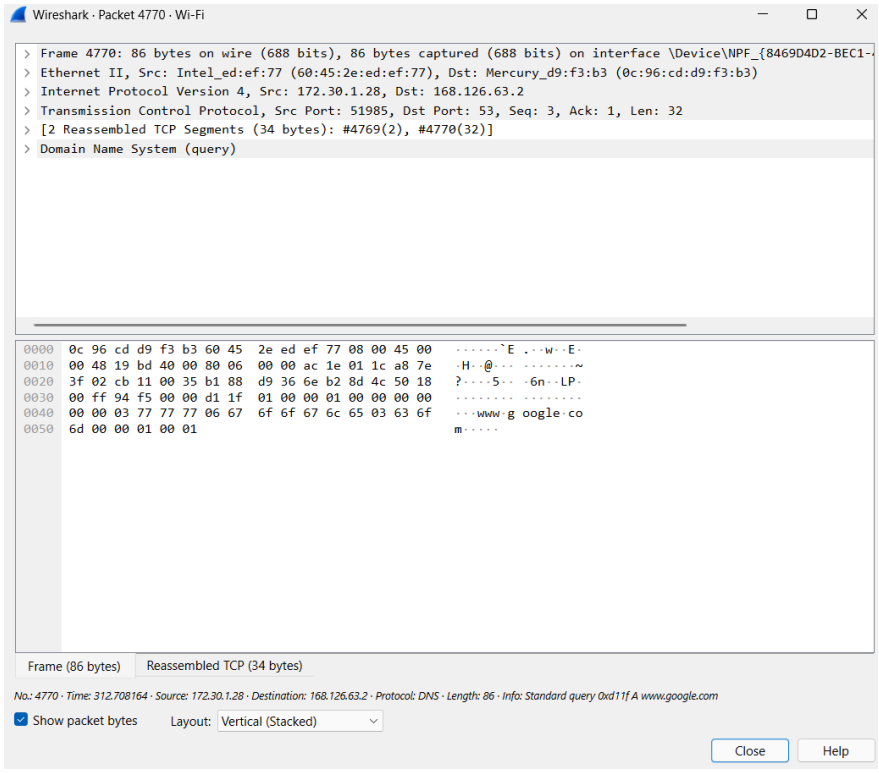
-응답 부분 (Answer Section): 질의에 대한 응답으로, 도메인 이름, IP 주소, 레코드 유형, 레코드 유효 기간 등이 포함된다.

-이름 서버 부분 (Name Server Section): 도메인을 관리하는 이름 서버의 정보를 포함한다.

-추가 레코드 부분 (Additional Records Section): 질의에 대한 추가적인 정보를 포함할 수 있다.

V. 실제 패킷 예시 분석: 패킷 분석 도구 **Wireshark**를 활용하여





Wireshark를 실행하여 Wi-Fi로 연결하고 Filter 입력창에 DNS를 입력해 DNS 관련 패킷만 보이도록 설정했다. 위 사진은 'www.google.com'으로 도메인 요청을 유도하여 캡쳐한 이미지이다.

Wireshark

Wireshark는 네트워크 패킷 분석기로, 캡처한 패킷 데이터를 상세하게 보여준다. 대표 기능으로는 네트워크 인터페이스로부터의 실시간 패킷 데이터 캡처, tcpdump/WinDump, Wireshark 및 기타 다양한 패킷 캡처 프로그램으로부터 저장된 파일 열기 등이 있다. 주로 네트워크 엔지니어는 네트워크 문제를 해결하고 보안 문제를 검사하기 위해 사용하고, 개발자는 프로토콜 구현을 디버깅하기 위해 사용한다. 그 외에도 네트워크 프로토콜 내부 동작을 공부하는 목적으로도 사용되는 등 다양한 상황과 관계자에 의해 사용된다.

오픈소스 소프트웨어이며, GNU 일반 공중 사용 허가서(GPL) 하에 배포된다. 모든 소스코드는 GPL 하에 공개되어 있어 자유롭게 새로운 프로토콜을 플러그인 형태나 내장 형태로 쉽게 추가할 수 있다. 그러나 Wireshark는 침입 탐지 시스템(IDS)이 아니므로 네트워크에서 이상이 발생할 경우 자동으로 경고해주지 않는다. 단지 관련 정보에 대한 분석을 제공함으로써 실제로 침입 또는 문제가 발생했을 때, 무슨 일이 벌어졌는지 파악하는 데 도움을 줄 수 있을 뿐이다. 또한, Wireshark는 네트워크에 영향을 주지 않고 오직 측정만 한다. 패킷을 전송하거나 능동적인 작업을 수행하지 않는다는 특징이 있다. 단, 도메인 이름 해석은 기본적으로 활성화돼 있고 비활성화할 수 있다.

실제 패킷 예시 분석

캡쳐 화면에 따르면, Time 312.708164, Source 172.30.1.28, Destination 168.126.63.2, Length 86, Transaction ID 0x1d1f, Query Type A 등이 정보가 나와있다. 이는 도메인을 입력했을 때 발생한 DNS 질의 패킷이며, TCP를 통해 포트 53(DNS 포트)으로 전송된 요청이라는 것을 확인할 수 있다.

Frame 4770: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)

4770는 Wireshark에서 순서대로 부여한 패킷 번호이다. 네트워크 상에서 실제 전송된 길이가 86바이트 (688비트), 캡처된 길이도 86바이트인 것으로 보아 손실 없이 전체 패킷 캡쳐했다는 것을 알 수 있다.

Ethernet II, Src: Intel_ed:ef:77 (60:45:2e:ed:ef:77), Dst: Mercury_d9

이더넷 계층 정보를 나타내는 부분이다. 출발지 주소가 60:45:2e:ed:ef:77로 장치의 네트워크 어댑터를 의미하고, 도착지 MAC 주소는 0c:96:cd:d9:f3:b3으로 DNS 서버 주소를 의미한다.

Internet Protocol Version 4, Src: 172.30.1.28, Dst: 168.126.63.2

IP 계층 정보(IPv4)를 언급하는 부분으로, 출발지(사용자 컴퓨터) IP 172.30.1.28에서 도착지(DNS 서버 주소) IP 168.126.63.2로 전송됨을 보인다.

Transmission Control Protocol, Src Port: 51985, Dst Port: 53, Seq: 3

전송 계층 정보(TCP)로써, 출발지 포트가 51985, 도착지 포트가 53임을 뜻한다. TCP 시퀀스 번호는 3으로 데이터 흐름을 제어하기 위해 쓰인다.

[2 Reassembled TCP Segments (34 bytes): #4769(2), #4770(32)]

이 DNS 요청 메시지는 2개의 TCP 세그먼트로 나눠져 있었고, #4769과 #4770 프레임이 재조립되었다는 것을 보여주는 문장이다. 총 길이는 34바이트이다.

결론

네트워크 프로토콜 중 하나인 DNS에 대해 조사하고 분석하며 네트워크 프로토콜의 기본 개념뿐만 아니라 실증적 관점에서 전체 메커니즘을 이해할 수 있었다. 특히, 프로토콜 동작 과정을 시각화 해봄으로써 동작 원리를 깊이 있게 이해할 수 있었다.

네트워크 프로토콜은 데이터 서식 지정 및 처리를 위한 규칙 세트로써, 상이한 소프트웨어와 하드웨어를 프로토콜을 사용하여 서로 통신하게 할 수 있다는 점에서 매우 시사성이 강하다. 효율성과 신뢰성을 위해 계층으로 작동되는데 크게 응용 계층, 전송 계층, 인터넷 계층, 네트워크 접근 계층으로 나뉜다. 응용 계층 중 하나인 DNS는 사용자 서비스를 제공함으로써 중요한 역할을 하고 있으며, 앞으로도 사용자 수준 발전에 따라 중요성이 커질 것이다.