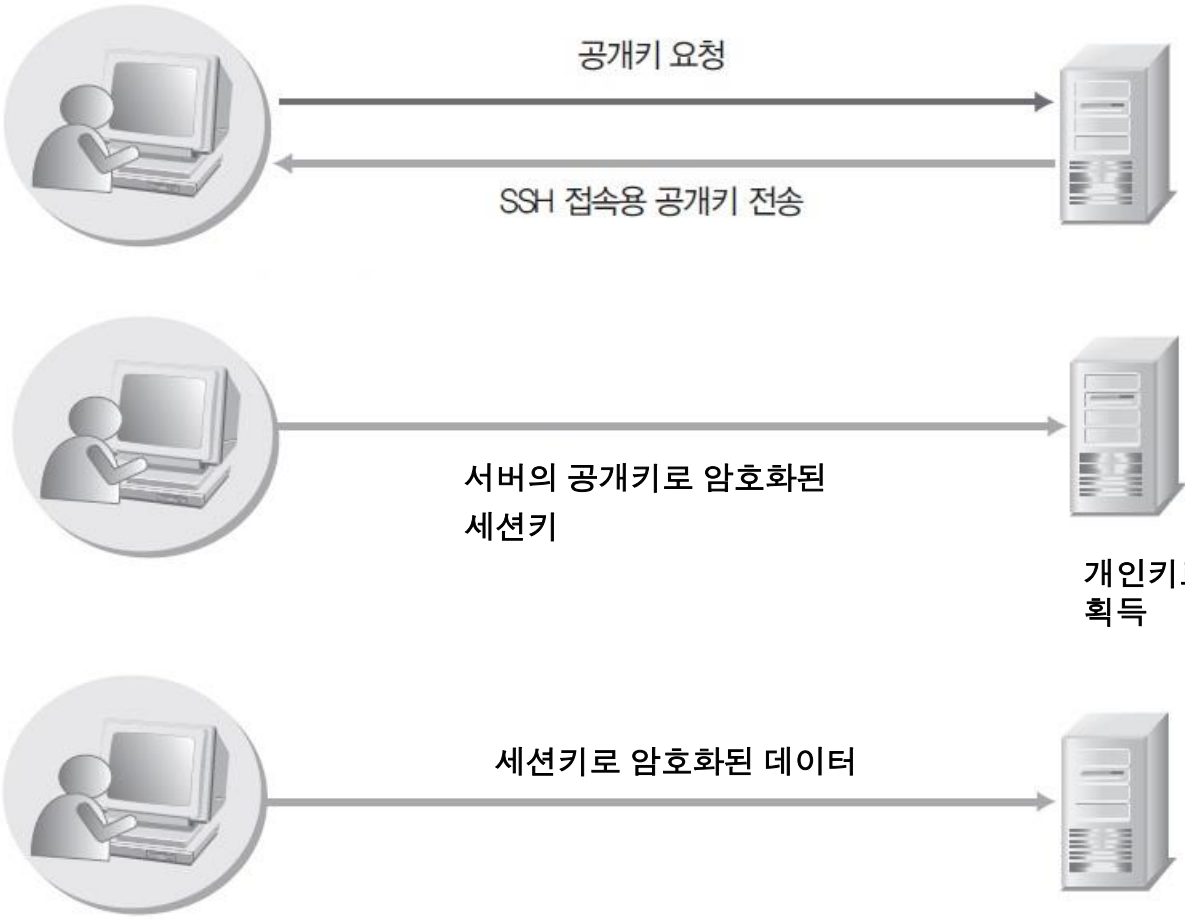
# SSL MITM

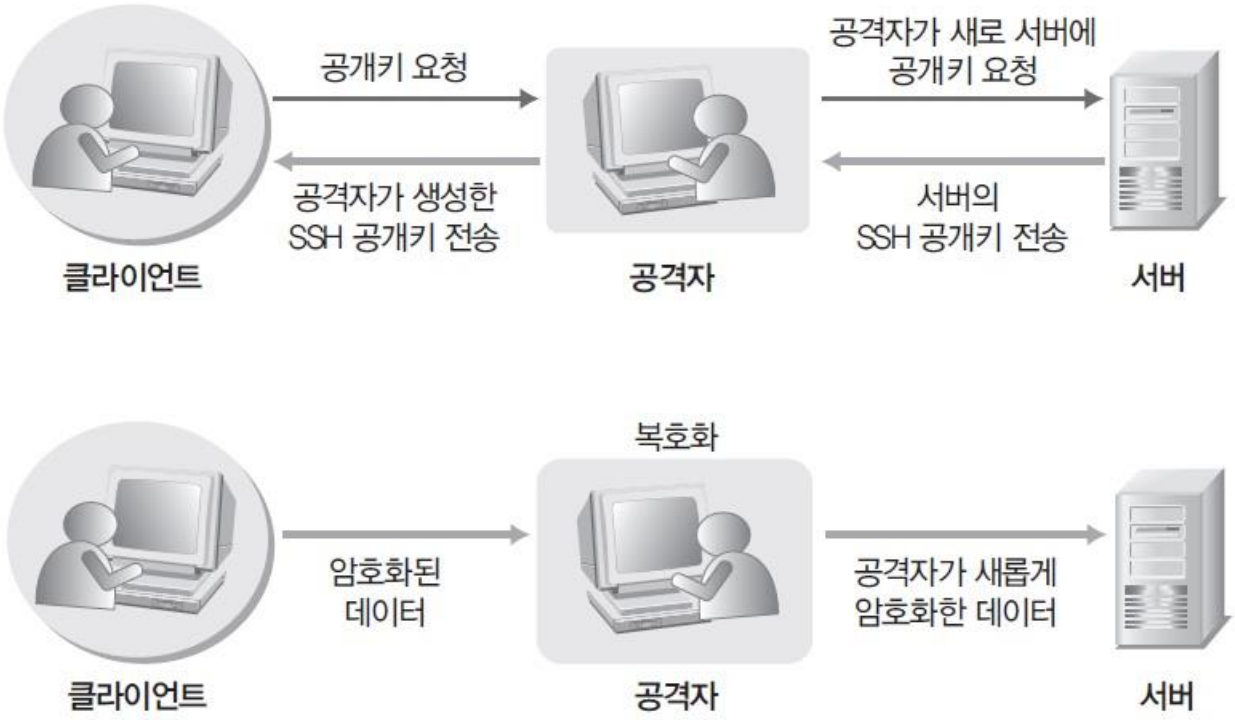
# MITM(MAN IN THE MIDDLE) 공격

- 통신 중간에 끼어들어 통신 상대방인 것처럼 속여 메시지를 도청하거나 위변조하는 공격

# SSH 접속 과정 REVIEW

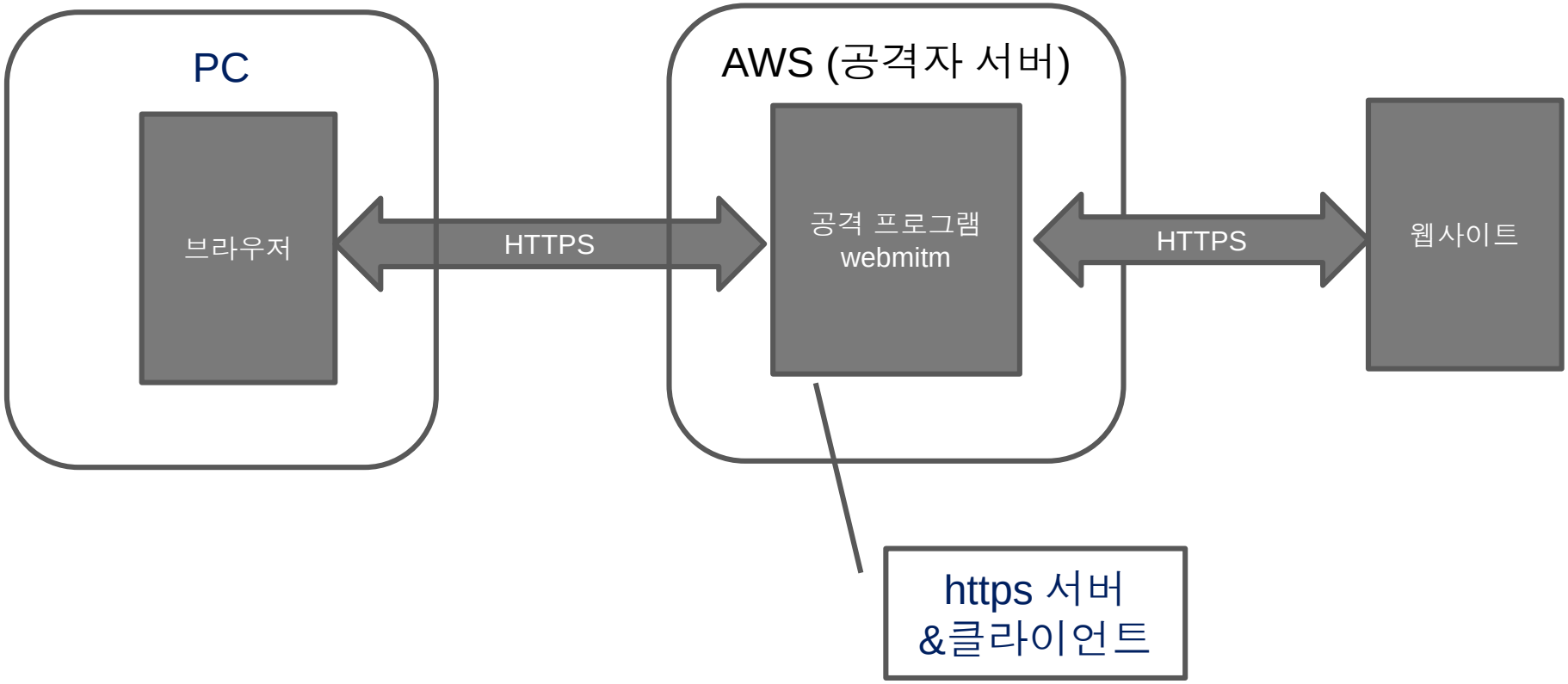


# SSH MITM


공개키 요청
공격자가 새로 서버에
공개키 요청
공격자가 생성한
SSH 공개키 전송
서버의
SSH 공개키 전송
클라이언트
공격자
서버
복호화
암호화된
데이터
공격자가 새롭게
암호화한 데이터
클라이언트
공격자
서버

# SSL MITM

- 가상 머신 사용하지 않음



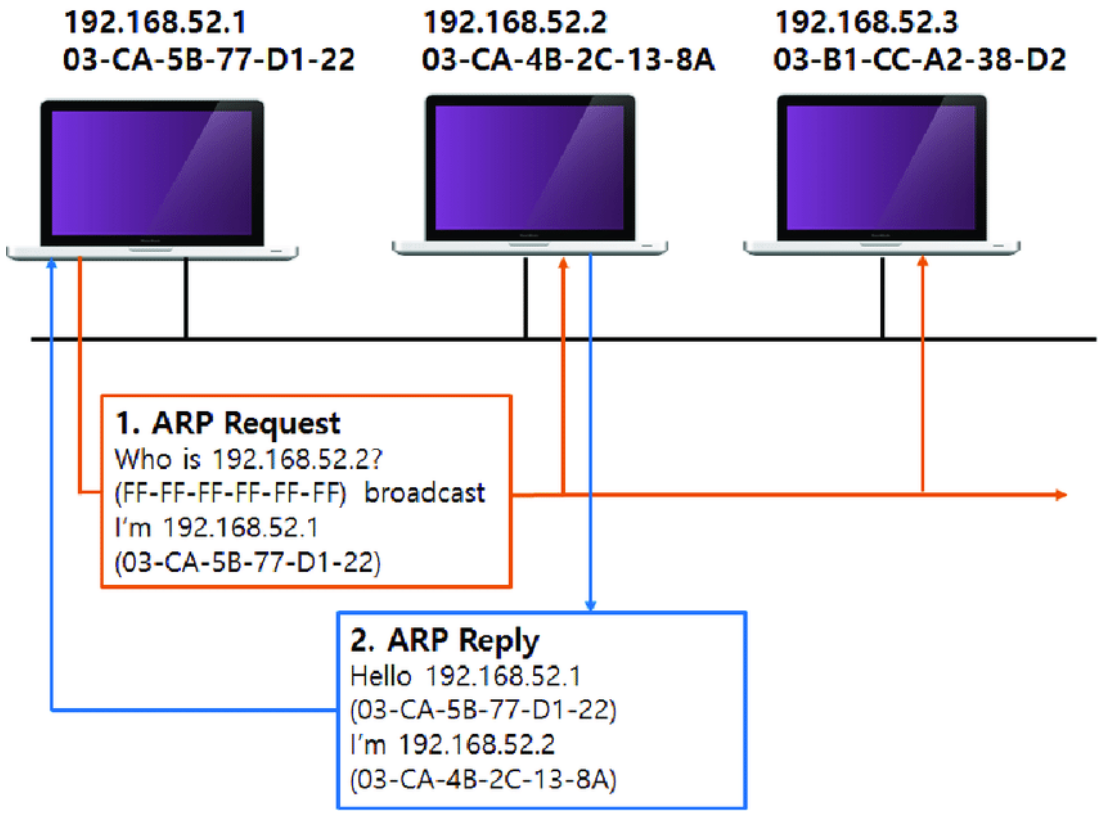
# MITM 로 유도하는 방법

- ARP 스푸핑
- DNS 스푸핑
- hosts 파일 변경
  - DNS 보다 먼저 참조하는 hosts 파일을 변경

# ARP스푸핑

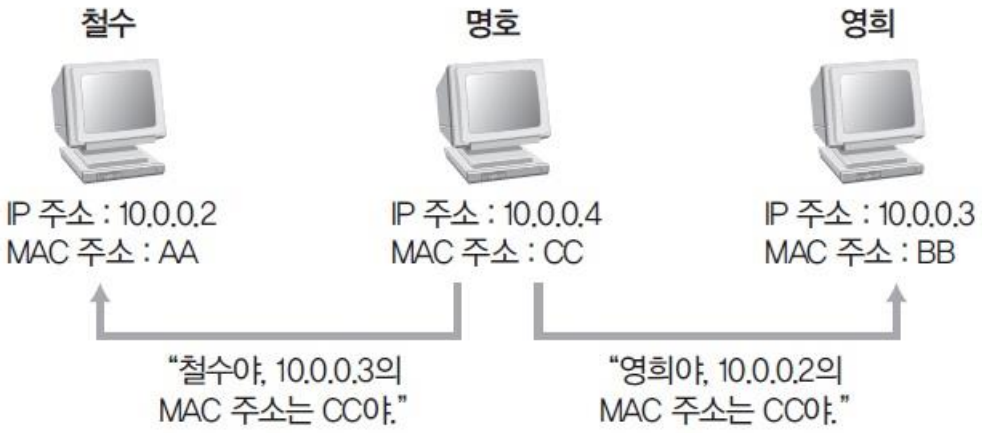
- ARP
  - IP⇔MAC주소
  - 조회

    CMD > arp –a



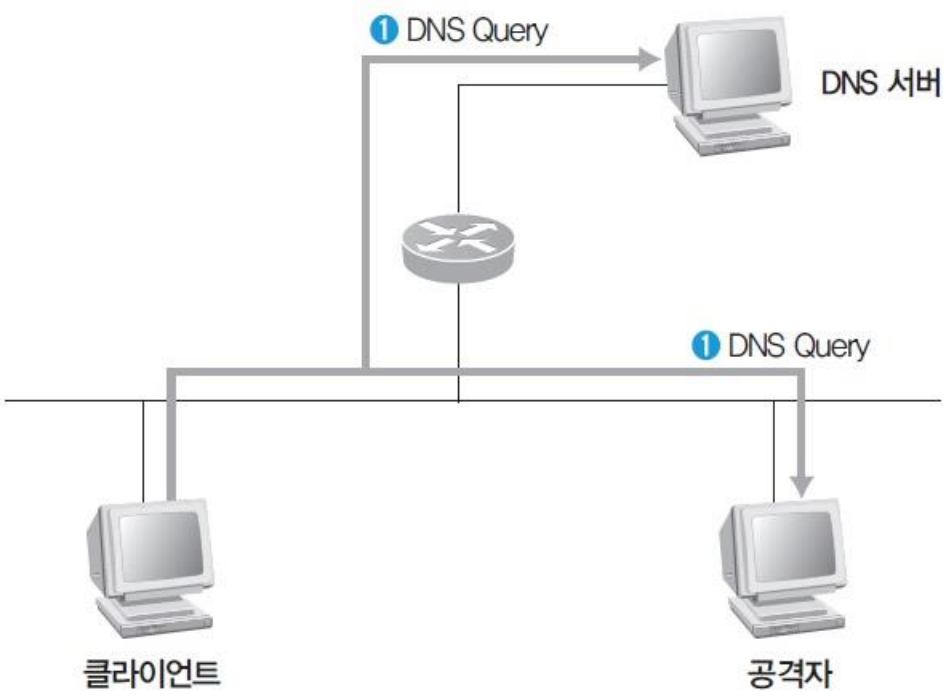
# ARP 스푸핑

## ARP 스푸핑



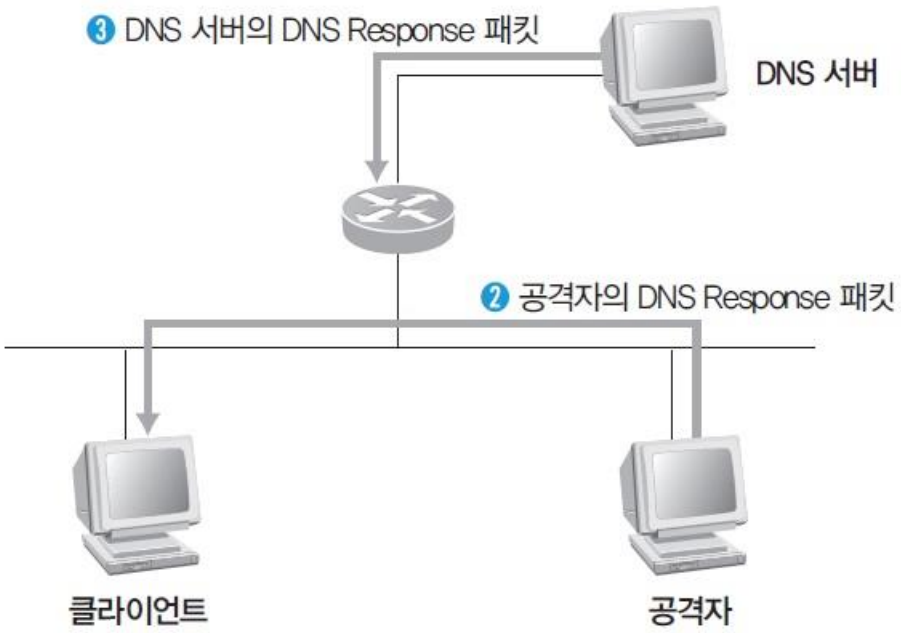
# DNS 스푸핑

① 클라이언트가 DNS 서버로 DNS Query 패킷을 보내는 것을 확인(ARP 스푸핑과 같은 선행 작업이 필요)



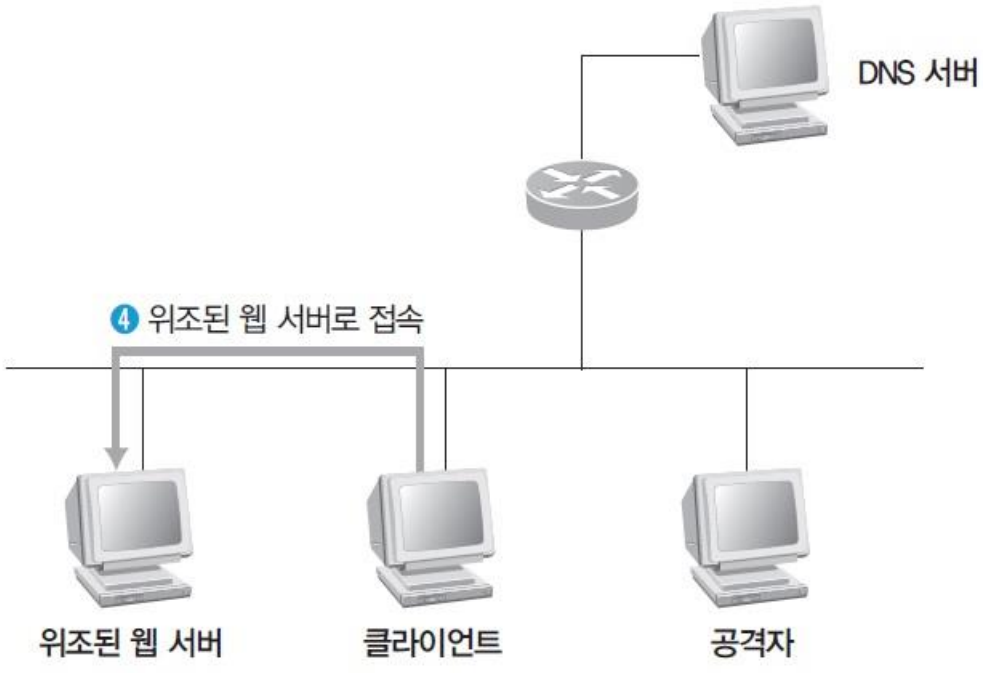
# DNS 스푸핑

② DNS 서버가 올바른 DNS Response 패킷을 보내주기 전에 위조된 DNS Response 패킷을 클라이언트에게 보냄



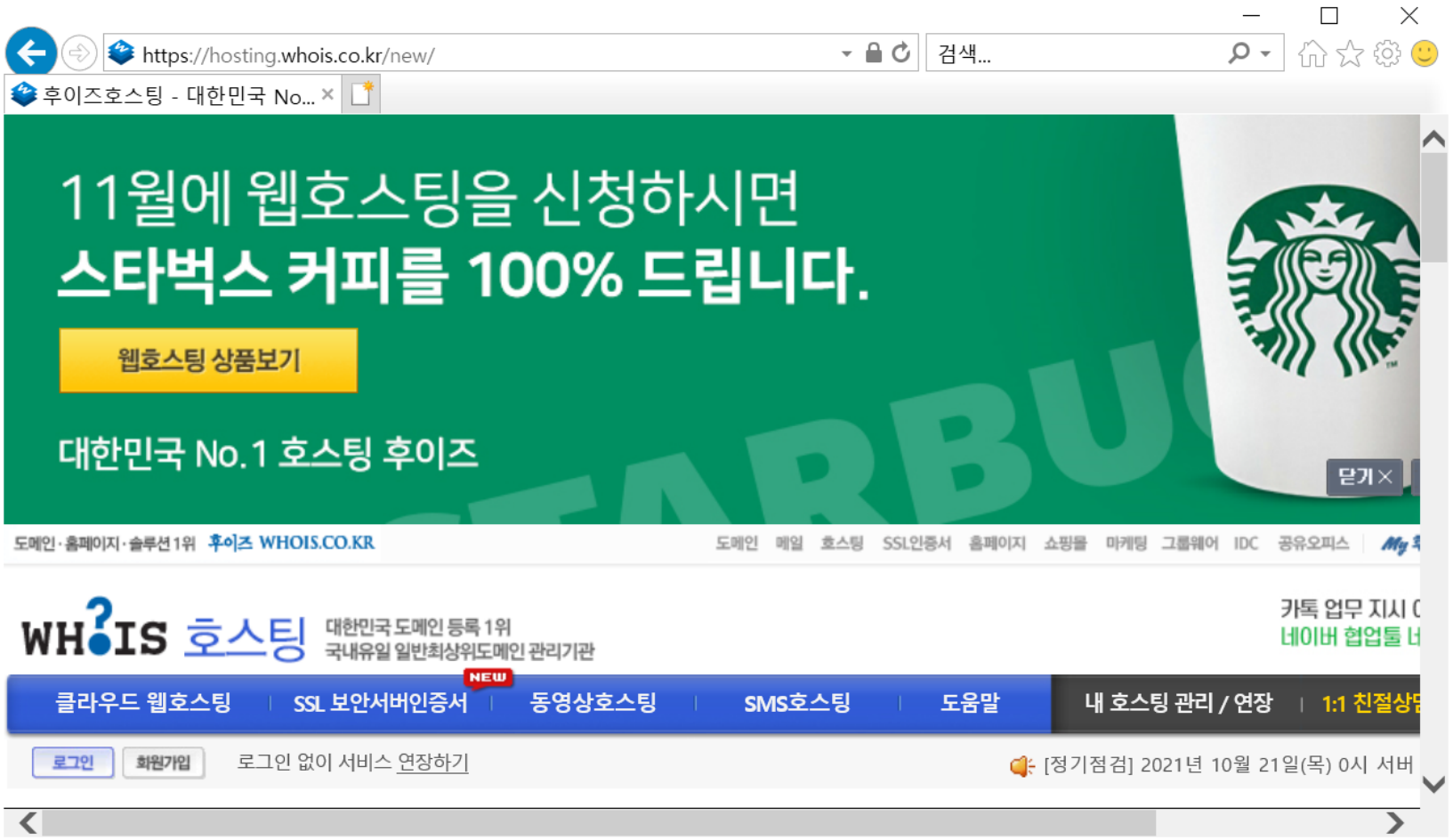
# DNS 스푸핑

③ 클라이언트는 공격자가 보낸 DNS Response 패킷을 올바른 패킷으로 인식하고 가짜 웹서버에 접속



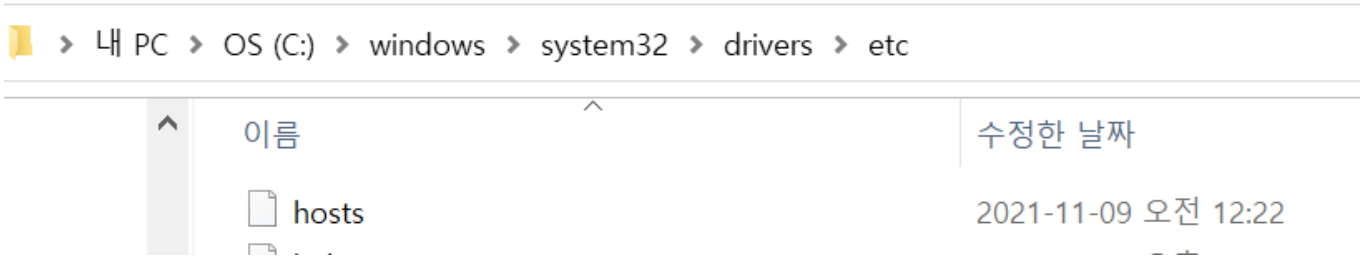
# SSL접속해 보기

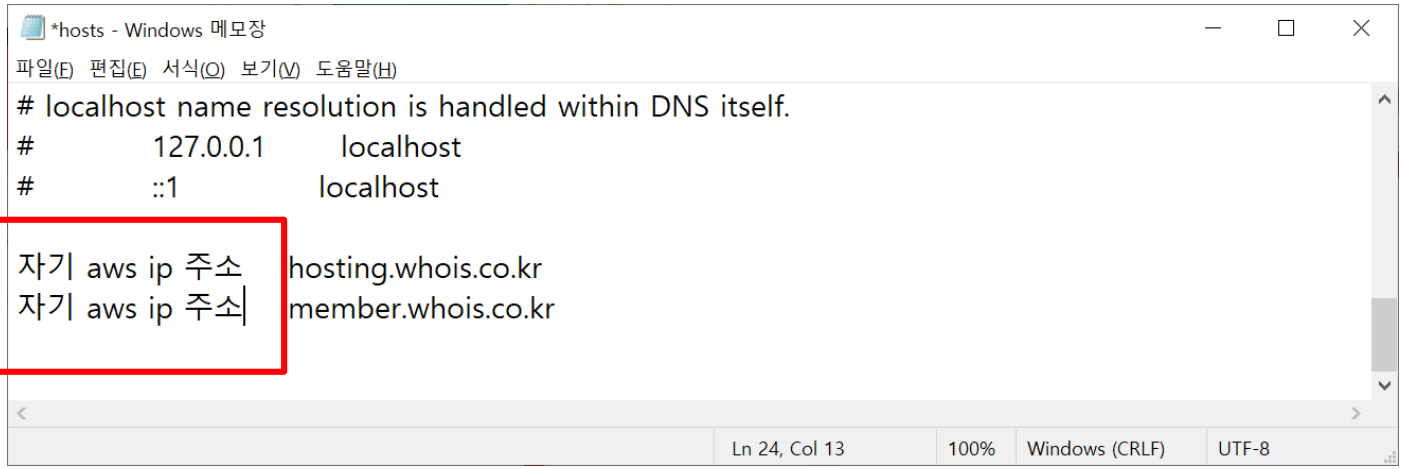
- hosting.whois.co.kr



# 윈도우즈 HOSTS파일 변경

- 변경 (관리자 권한) 후 접속해보기
  - 백신의 경고 무시
  - 브라우저 재실행 필요



# MITM 프로그램 설치, 실행

## dsniff

```
ubuntu@ip-172-31-13-205:~/10$ sudo apt install dsniff
```

## 실행

```
ubuntu@ip-172-31-13-205:~/10$ sudo webmitm
```

- 처음 실행시 SSL서버용 인증서 생성 : webmitm.crt
  - 키와 인증서 모두 포함
- 이후 실행 시 위 인증서 사용하여 웹서버처럼 동작

☞ 오류 발생, 키 길이 부족

# CA 키쌍 생성, 인증서 SS

- 서버 인증서 만들기
  - 저번 시간에 한 것이 있으면 이 페이지는 건너뜀
- openssl 간략화 도구 설치

  $ sudo apt install easyrsa
- 폴더 및  script 설치

  $ make-cadir ca
- pki 폴더 설치

  $ cd ca  ( 이후로 경로는 주욱 ~/ca $ )

  $ ./easyrsa init-pki
- CA 키쌍 생성 및 인증서

  $ ./easyrsa build-ca nopass

# 서버인증서 생성

- 서버 키 쌍, 인증요청서 생성 : CN은 자기 이름으로

  $ ./easyrsa gen-req server nopass

- 서버 인증서 발행

  $ ./easyrsa sign-req server 자기이름

- 인증서와 키 파일 내용 (PEM 부분) 을 ~$ webmitm.crt 의 PEM 부분에 overwrite 하기

  pki/private/자기이름.key

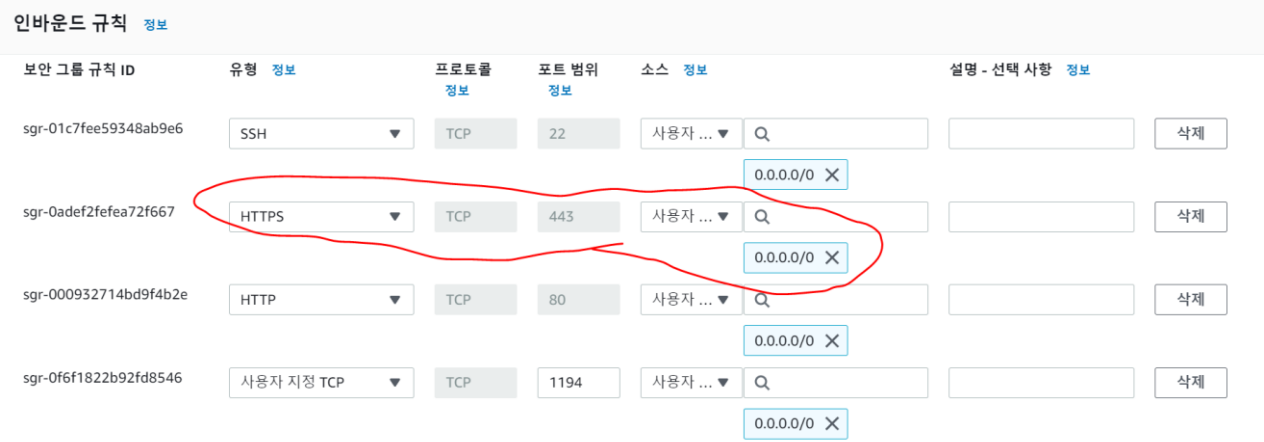
  pki/issued/자기이름.crt

# MITM 실행 및 포트 열기

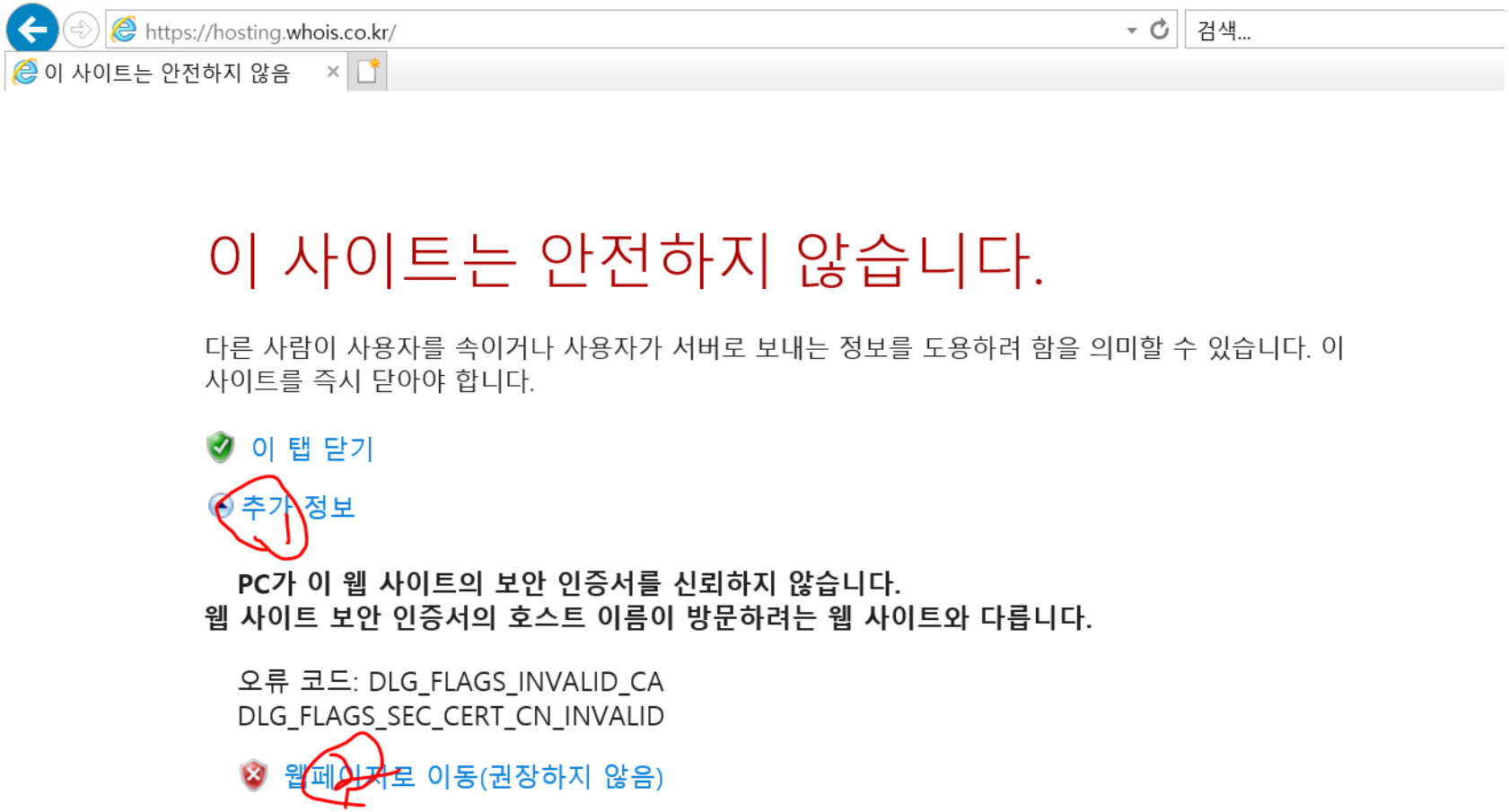
- webmitm 실행

```
ubuntu@ip-172-31-13-205:~/10$ sudo webmitm
webmitm: relaying transparently
```

- AWS https 포트 개방



# 다시 접속하기


https://hosting.whois.co.kr/
검색...
이 사이트는 안전하지 않음
이 사이트는 안전하지 않습니다.
다른 사람이 사용자를 속이거나 사용자가 서버로 보내는 정보를 도용하려 함을 의미할 수 있습니다. 이 사이트를 즉시 닫아야 합니다.
이 탭 닫기
추가 정보
PC가 이 웹 사이트의 보안 인증서를 신뢰하지 않습니다.
웹 사이트 보안 인증서의 호스트 이름이 방문하려는 웹 사이트와 다릅니다.
오류 코드: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID
웹페이지로 이동(권장하지 않음)

# SSL서버 인증서 오류 2가지

- 신뢰하지 못하는 CA가 발행
- CN domain name 과 같아야 함

# 과제1

- 직전 페이지 인증서 내용 cn 자기이름 나오게 캡처
- 1.jpg

# 피싱, 파밍

- 여기까지가 가짜 웹사이트로 유도되는 피싱, 파밍과 같음
- 차이점
  - 피싱, 파밍은 가짜 사이트를 만들어서 운용
  - MITM은 진짜 사이트를 중계
  - MITM 피싱은 relay 이기 때문에 모든 인증 수단을 중계할 수 있다.
    - 대응 방안은 지정 단말
    - -> IP spoofing , MAC spoofing 에 의해 무력화됨

# 패킷 내용 보기

- ssldump

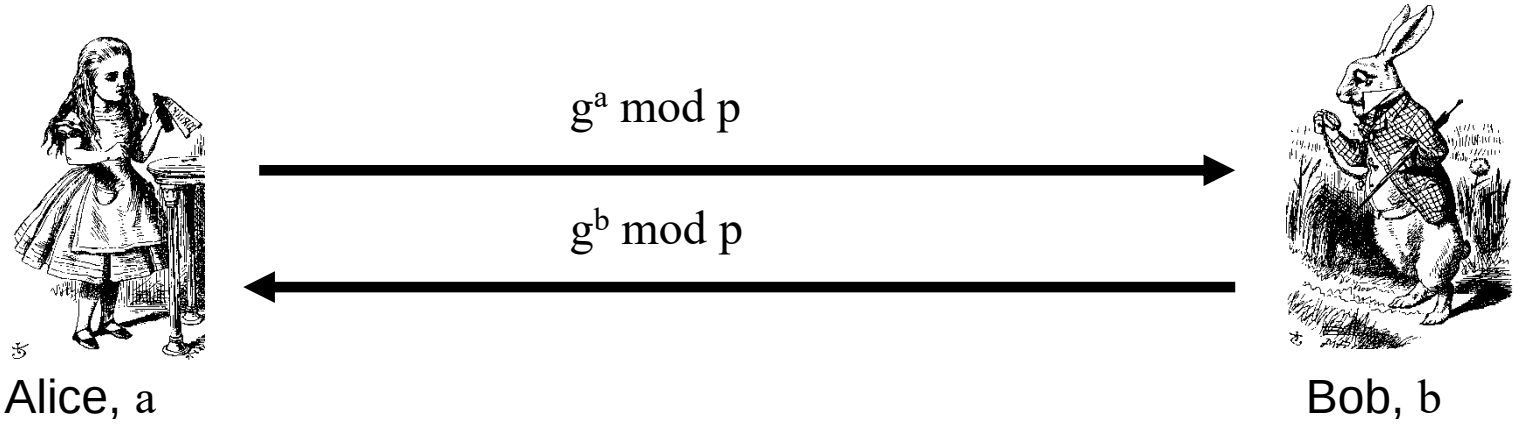
```
ubuntu@ip-172-31-13-205:~/10$ sudo apt install ssldump
```

- ssl packet dump

```
ubuntu@ip-172-31-13-205:~/10$ sudo ssldump -i eth0  -k webmitm.crt -d
```

# EPHEMERAL DIFFIE-HELLMAN

- 패킷 캡처한 것으로는 복호화 불가능




☞ webmitm에서 decrypt packet을 출력해야

# 과제2

- 서버 인증서 cn을 도메인 이름과 맞추고,
  - 추가로



- CA인증서를 가져와서 trust list 에 넣은 후 사이트 접속 결과 확인하기
  - 브라우저 창에 어떻게 표시되는지 확인
- 2.jpg