# DNS와 SNI를 이용한 인터넷 검열

윤재웅 * 김경호 * * 서화정 * *†

*한성대학교 컴퓨터공학부
**한성대학교 대학원 IT융합공학부

## 요 약

● 불법 사이트 차단을 명분으로 진행중인 인터넷 검열이 표현의 자유를 억압

● 올해 2월부터 TLS 확장인 SNI 필드를 통한 검열이 진행 중

● DNS, HTTP, SNI의 차단 및 암호화 방식에 대한 동향


fig 1. 아시아 지역의 인터넷 차단

## DNS 차단

● 클라이언트의 요청을 파밍(Pharming)을 이용하여 ‘Warning’ 사이트로 리다이렉션

● DNS 차단은 해외 DNS 서버를 통한 우회 가능

● DNS 암호화 방식

- DNSSEC : DNS 서버 내부적으로 사용하는 DNS 정보 유효성 검증 절차.
- DNS over HTTPS : DNS 서버와 HTTPS 방식으로 보안통신하여 DNS 정보를 가져오는 방식. (port. 443)
- DNS over TLS : DNS 서버와 TLS 보안 통신을 하여 DNS 정보를 가져오는 방식. (port. 853)

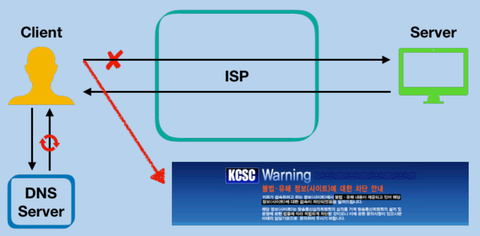


fig 2. DNS 차단 방식

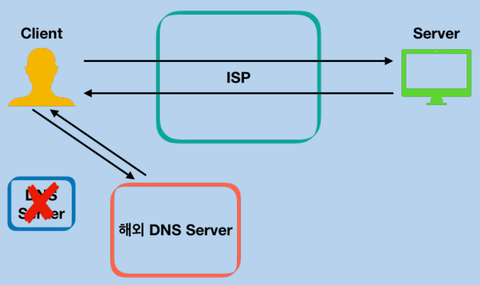


fig 3. 해외 DNS를 통한 차단 우회

## HTTP 차단

● 암호화 되지 않은 평문으로 통신한다.

● 해외 DNS로부터 IP 주소를 수신해도 ISP에게 해당 주소를 요청 시 차단 방식

● TLS(Transport Layer Security)로 암호화한 HTTPS를 통한 차단 우회

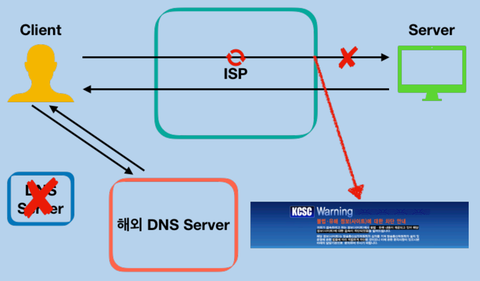


fig 4. HTTP 차단 방식

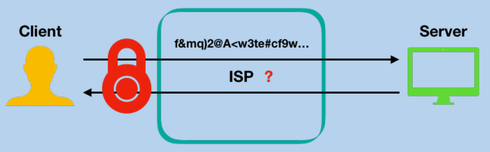


fig 5. HTTPS를 통한 차단 우회

## SNI 차단(HTTPS 차단)

● 웹 서버에서 여러 도메인의 웹 사이트를 서비스하는 경우에도 인증서를 사용한 HTTPS 사용을 가능하게 함

● HTTP를 암호화 하기 전 ClienHello 패킷에서 평문 노출

● TLS 1.3에서 SNI암호화인 ESNI(Encryption SNI) 제안 (드래프트)

- 암호화된 DNS 통신을 이용하여 공개키 배포, 이 공개키를 이용한 SNI 암호화

● HTTPS 기반의 웹 서버와 DNS 서버 상호간의 동기화 문제점 존재

- SNI 암호화에 사용되는 키의 만료기간으로 인한 갱신

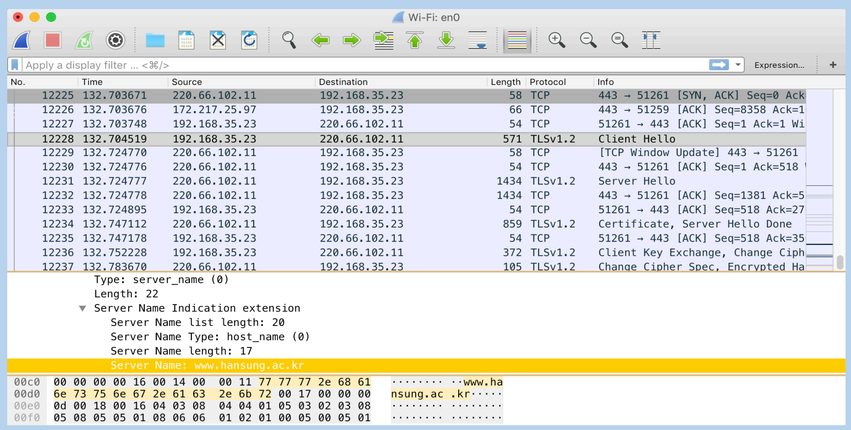


fig 6. SNI의 평문 노출