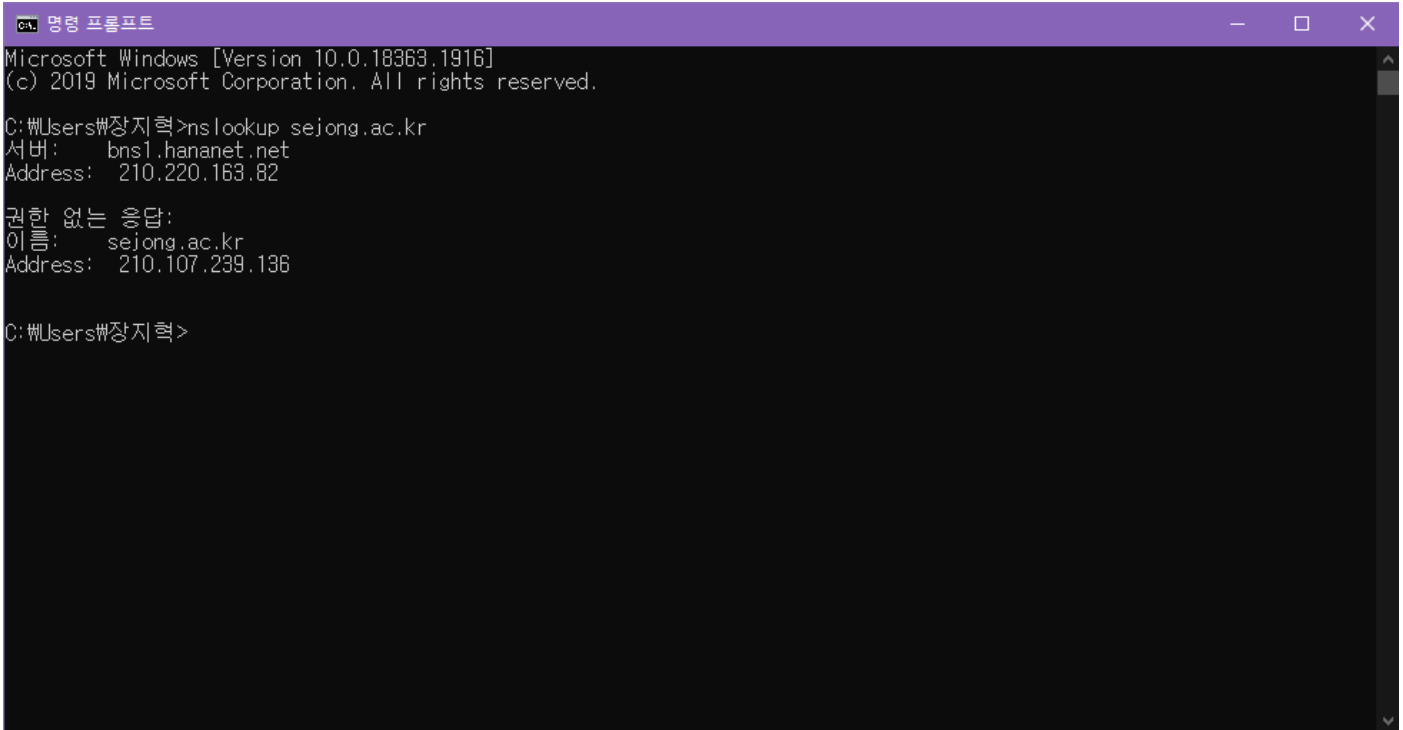


11.1 과제 주제

cmd 상에서 nslookup sejong.ac.kr 를 통해 얻은 IP 주소로 접속한 후 화면 캡처하기



```
CA 명령 프롬프트
Microsoft Windows [Version 10.0.18363.1916]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\장지혁>nslookup sejong.ac.kr
서버:      bns1.hananet.net
Address:  210.220.163.82

권한 없는 응답:
이름:      sejong.ac.kr
Address:  210.107.239.136

C:\Users\장지혁>
```

11.2 과제 주제

정상적인 DNS 과정과 DNS 캐시 포이즌 공격 과정의 차이 설명하기

URL 을 웹브라우저에 입력했을 때 이 URL 이 DNS 캐시에 저장되어 있으면 해당 IP 주소를 바로 반환하고 저장되어 있지 않다면 다른 DNS 서버에게 물어봐서 IP 주소를 가져오게 되는 과정이 정상적인 DNS 과정이다.

DNS 캐시 포이즌 공격은 DNS 캐시 메모리에 가짜 데이터를 저장해 클라이언트의 요청시에 변조된 웹사이트 IP 를 전송하는 공격수단이다. DNS 캐시 포이즌 공격을 통해 공격자는 개인정보 탈취, Malward 유포 등을 수행하게 된다.

11.3 과제 주제

파밍 공격과 관련되 사건 및 사례조사

https://news.jtbc.joins.com/article/article.aspx?news_id=NB10659720 (JTBC 뉴스 14/11/27)

은행 댁은꼴 사이트'로...파밍 피해액, 올해만 642 억

피해자가 인터넷 뱅킹을 위해 은행 홈페이지 접속 후, 보안을 강화하라는 메시지에 개인정보를 입력했더니 며칠 뒤에 계좌에서 돈이 빠져나간 파밍 사건이다.

범죄자들이 컴퓨터에 악성코드를 심고 피해자가 은행에 접속할 시 가짜 금융기관 사이트에 연결되도록 한 후 개인정보를 탈취하는 방식으로 공격을 시행했다. 실제 홈페이지와 가짜 사이트가 똑같아 보이기 때문에 파밍 피해를 당하지 않기 위해서는 OS, 백신 업데이트를 꾸준히 해주어야 한다.

11.4 과제 주제

피싱 공격과 관련되 사건 및 사례조사

<https://www.hankookilbo.com/News/Read/A2021110508400003707> (한국일보 21/11/05)

“요소수 팔아요” 통화뒤 8000만원 입금했는데...보이스피싱이었다

요소수 품귀 현상을 악용하여 보이스 피싱을 한 사건이다. 공격자들은 KT 를 사칭하며 요소수 업체에 전화를 해서 회선공사를 이유로 사무실 전화를 착신전환 하도록 시켰고, 그 시간 동안 요소수 구매를 희망하여 업체에 전화를 한 구매자들의 돈을 본인들의 계좌에 입금시키게 했다.