16011069 장지혁

9.1 과제 주제

스푸핑, 스누핑, 스니핑의 차이에 대해 조사하기

1. 스푸핑

스푸핑(spoofing)이라는 단어는 눈속임(spoof)에서 파생된 IT 용어이며, 직접적으로 공격자가 시스템에 침입을 하지는 않지만, 피해자가 **공격자의 악의적인 시도에 의한 잘못된 정보, 혹은 연결을 신뢰하게끔** 만드는 일련의 기법들을 의미한다. 피싱이나 스니핑과는 달리 더욱 적극적으로 피해자의 시스템이 잘못된 정보를 신뢰하고 받아들이게끔 유도하며, 피해자는 자신이 속고 있음을 알아채기 힘들다. 종류에는 DNS 스푸핑, ARP 스푸핑, IP 스푸핑이 있다.

2. 스누핑

스누핑(snooping)은 염탐하다라는 뜻을 갖고 있다. 스누핑은 프로토콜 분석용 소프트웨어를 지칭하며 **네트워크상에 떠도는 중요 정보들을 몰래 획득하는 행위**를 말한다. 종류에는 IGMP 스누핑, DHCP 스누핑이 있다.

3. 스니핑

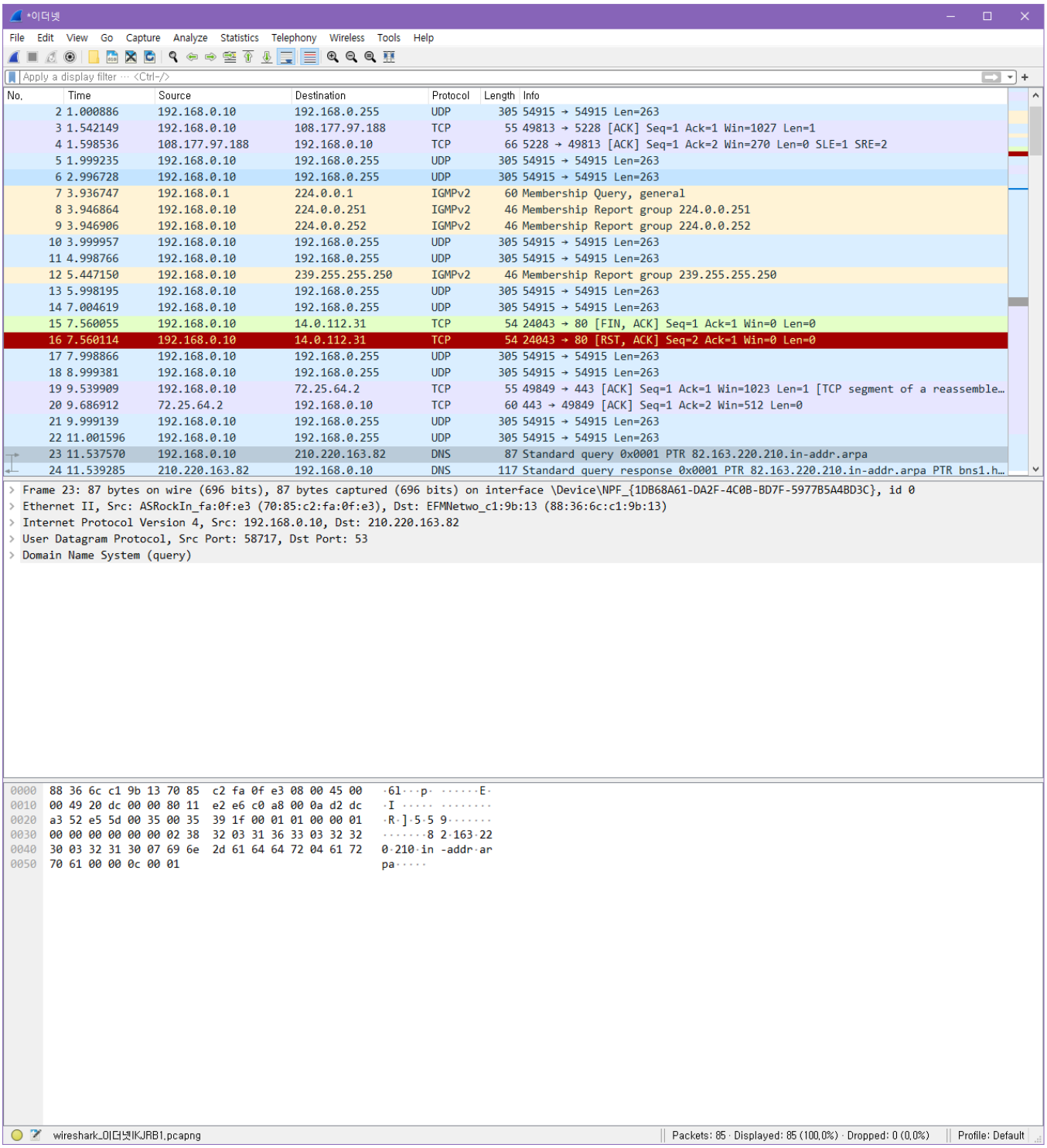
스니핑(sniffing)은 **네트워크상의 데이터를 도청하는 행위**를 말한다. 공격할 때 아무것도 하지 않고 조용히 있는 것만으로도 충분하기 때문에 수동적인 공격이라고도 한다. 일반적으로 스니핑 공격은 IP 주소 필터링과 MAC 주소 필터링을 수행하지 않고 랜카드로 들어오는 전기신호를 모두 읽어 관찰하여 정보를 유출시키는 것을 의미한다.

스푸핑은 **공격자의 악의적인 시도에 의한 잘못된 정보나 연결을 신뢰하게끔 만드는 기법**들로 사용자들을 유도하여 정보를 빼가는 해킹 수법이라고 할 수 있다.

스누핑은 **네트워크 상에 떠도는 중요 정보를 몰래 획득하는 행위**이며 **스니핑**은 **패킷교환을 엿보는, 도청하는 행위**라고 할 수 있다. 즉 스니핑은 패킷교환을 훔쳐보는 행위에 그치지만, 스누핑은 중요 정보를 획득하는데 초점이 맞춰져 있다고 볼 수 있다.

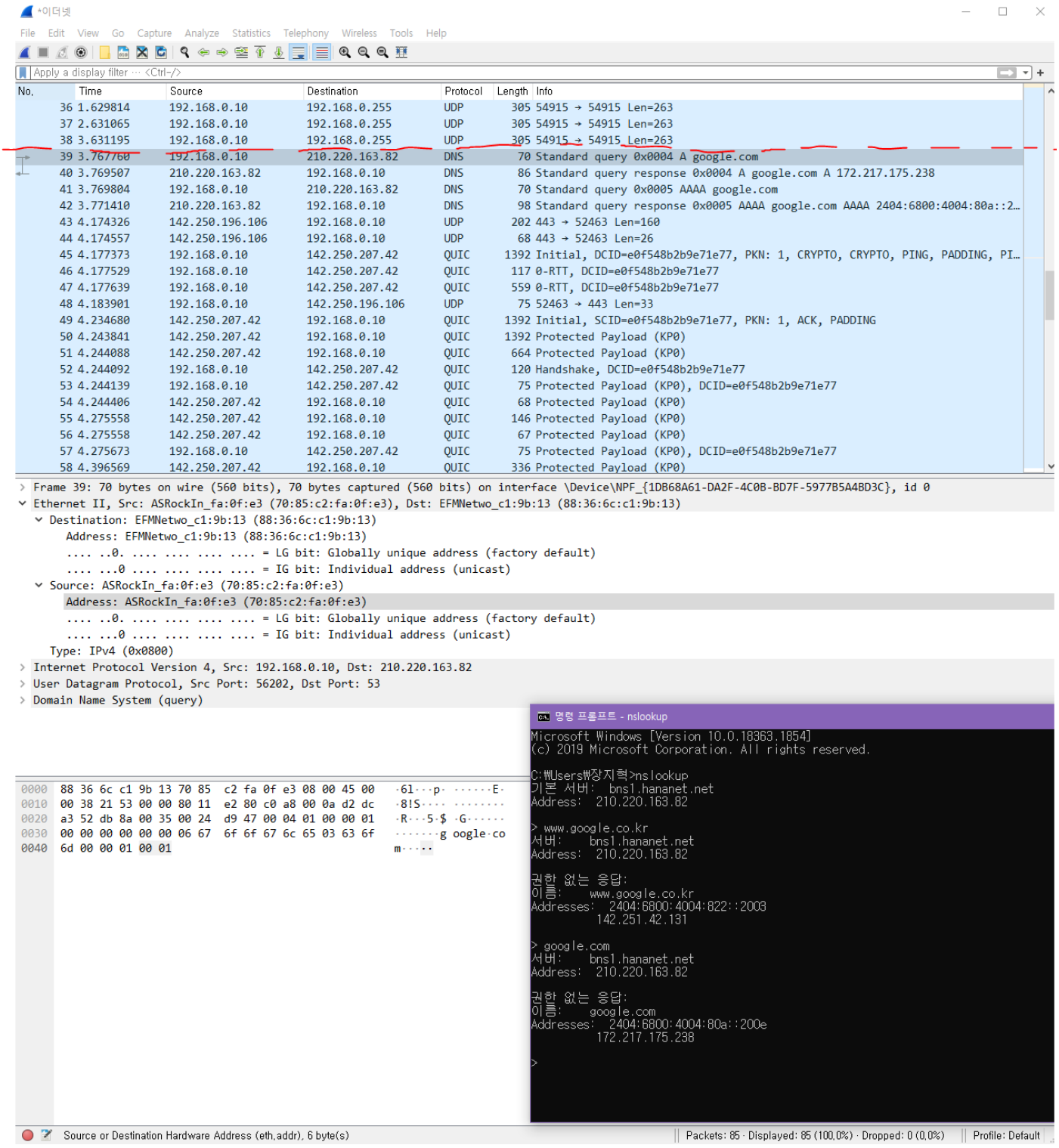
9.2 과제 주제

WireShark 를 사용하여 본인의 네트워크 인터페이스로 송/수신 되는 패킷들을 보여주는 패킷 List, 그리고 임의의 패킷 하나를 선택하여 상세 내용을 보여주는 화면을 캡쳐하기 (List, Details, 패킷 Bytes 가 보이도록 캡펴할 것)



9.3 과제 주제

cmd 상에서 입력한 nslookup 과 WireShark 를 사용하여 www.google.com 명령 실행한 결과 캡쳐하기



빨간 선이후 DNS 와 패킷을 교환하는 기록 시작