**[REPORT – 실습6]**

**-9주차 Wireshark-**



**과 목 명 : 컴퓨터보안 - 02**

**교 수 : 김영부 교수님**

**학번 : 2020112119**

**이름 : 강동희**

**제출일 : 2023.04.11**

**목 차**

1. **서론**
   1. 문제 정의
   2. 문제 분석
2. **본론**
   1. Wireshark 설치 및 기능
   2. 실습 1 : 패킷 가지고 놀기
   3. 실습 2 : Wireshark를 이용한 패킷 분석
   4. 실습 3 : ICMP 패킷 디코딩 수행
   5. 실습 4 : TraceRoute
3. **결론**
   1. 실습 결과 및 분석
   2. 고찰(Discussion)

**APPENDIX**

A. 소스 코드

1 서 론

1.1 문제 정의  
1. Wireshark 설치 및 기능

와이어샤크는 오픈소스 패킷 분석 프로그램이며, 네트워크의 문제, 분석, 소프트웨어 및 통신 프로토콜 개발, 교육에 쓰인다.

2. 실습 1 : 패킷 가지고 놀기

3. 실습 2 : Wireshark를 이용한 패킷 분석

4. 실습 3 : ICMP 패킷 디코딩 수행

5. 실습 4 : Trace Route

* 1. 문제 분석

1. 본 론

2.1 와이어샤크 설치 및 기능

와이어샤크는 오픈소스 패킷 분석 프로그램으로 네트워크의 문제, 분석, 소프트웨어 및 통신 프로토콜 개발 등을 위해 사용할 수 있다. 주로 “pcap”을 이용하여 패킷을 잡아내는 것이 주요 기능이다. Promiscuous mode(무차별 모드)를 지원하여 통신이 되는 모든 패킷을 얻을 수 있으며, broadcast와 multicast 트래픽 또한 얻을 수 있다. 실습 진행을 위해서 Stable release 버전인 4.0.5 버전을 설치하였다. (그림1)

텍스트이(가) 표시된 사진

자동 생성된 설명

그림 1. 와이어샤크 설치 및 버전 확인

와이어샤크를 설치 후 실행하게 되면 다음 그림2와 같은 인터페이스 화면이 나타나게 된다. 해당 화면에서는 현재 내 컴퓨터가 통신하고 있는 와이파이, 이더넷 등 패킷 캡처를 위한 종류를 선택할 수 있게 된다. (현재는 wifi로 연결되어 있으므로 Wi-Fi를 선택한다.

텍스트이(가) 표시된 사진

자동 생성된 설명

그림 2. 와이어샤크 실행 후 인터페이스

다음 그림 3은 와이어샤크 메인 인터페이스로 실시간으로 패킷을 확인할 수 있으며 다음과 같은 정보들을 확인할 수 있다.

No(패킷을 수집한 순서), Time(패킷이 수집된 시간), Source(패킷을 보낸 주소) Destination(패킷 도착 주소), Protocol(프로토콜 정보), Length(패킷의 길이) Info(패킷 정보)

텍스트이(가) 표시된 사진

자동 생성된 설명

그림 3. 메인 인터페이스

와이어샤크의 실행 과정을 확인해보기 위해 직접 특정 서버(네이버)에 ping을 보내 해당 패킷이 와이어샤크에 잡히는지 확인해보았다. 먼저 **nkslookup 명령어**를 통해 네이버의 Ip주소를 확인하고(223.130.220.104) 해당 주소로 **ping 명령어**를 통해 ping을 전송한다. (그림 4) 이때 와이어샤크는 실행 중이어야 한다.

텍스트이(가) 표시된 사진

자동 생성된 설명

그림 4. 네이버 서버로 ping 전송

그림 4와 같이 ping을 전송했다면 와이어샤크에는 다양한 패킷 정보들을 수집되어 있다. 이때, 특정 ip주소의 패킷만 확인하기 위해 filter를 사용한다. Ip주소에 대한 필터링을 수행하기 위해서는 ip addr 이라는 명령어 뒤에 조건 연산자와 함께 Ip주소를 입력한다. (그림5)

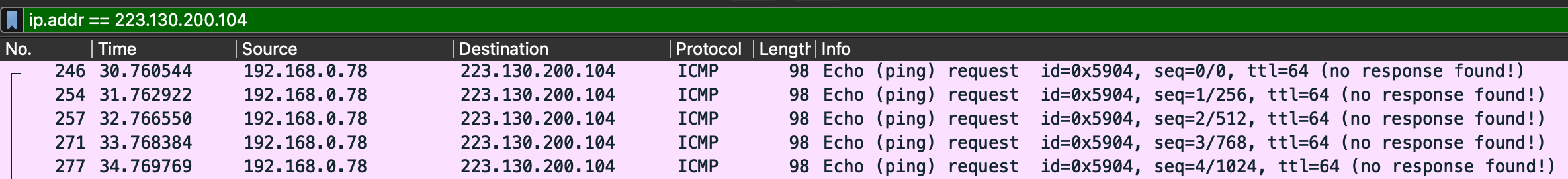


그림 5. 223.130.220.104의 패킷 수집 정보

이로써 와이어샤크에 대한 정보를 비롯해 수행 과정, 분석할 수 있는 정보들을 확인할 수 있었다.

* 1. 실습 1: 패킷 가지고 놀기

1. 아래 그림을 조사해보고 Packet1와 packet2의 운영체제가 무엇인지 추축 해보시오.

텍스트이(가) 표시된 사진

자동 생성된 설명 텍스트이(가) 표시된 사진

자동 생성된 설명

그림 6. Packet1. 그림 7. Packet2

위 두 그림은 ping을 통해 운영체제를 식별할 수 있다는 점을 알 수 있다. 그림의 특징을 정리해보면 Packet1을 통해 알 수 있는 점은 다음 표1 과 같다.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Fragment offset | **0** | TTL | **64** | Protocol | **TCP** | Window size value | **2956** | Window size | **2956** |

표 1. Packet1의 정보

또한 Packet2를 통해 알 수 있는 점은 다음 표2와 같다.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Fragment offset | **0** | TTL | **128** | Protocol | **TCP** | Window size value | **16344** | Window size | **16344** |

표 2. Packet2의 정보

먼저 ‘ping’에 대해 알아보자면 네트워크 통신을 테스트하는 데 사용되는 도구로 destination 호스트로 ICMP(Internet Control Message Protocol) Echo 요청을 보내고, 해당 호스트로부터 응답을 받는다. 이를 통해 네트워크의 가용성을 비롯해 시간을 측정 및 평가할 수 있다.

‘ping’ 명령은 여러 운영체제에서 사용할 수 있으며, 응답 패킷에 포함된 Time to live(TTL) 값은 호스트의 운영 체제를 식별하는 데 확인한다. TTL은 IP 패킷이 네트워크TT를 통과할 때마다 감소하는 값으로 패킷이 무한 루프에 빠지는 경우를 방지하기 위해 사용된다는 것을 알 수 있다.

대표적으로 TTL의 값에 따른 운영체제를 정리하면 다음과 같다.

|  |  |
| --- | --- |
| Linux | 64 |
| Windows | 128 |
| Cisco | 256 |

표 3. 운영체제(OS)에 따른 TTL 값

한편 ‘window size’는 네트워크 통신에서 사용되는 TCP(Transmission Control Protocol) 패킷의 윈도우 크기를 지정하는 매개변수이다. TCP는 신뢰성 있는 데이터 전송을 위해 사용되며, 데이터를 작은 패킷으로 분할하여 전송합니다. 윈도우 크기는 한 번에 전송할 수 있는 패킷의 수를 결정하며, 네트워크의 대역폭과 지연 시간에 따라 조절된다. 따라서 Packet1은 Linux, Packet2는 Windows 이다.

2. 아래의 그림을 조사해보고 보안 문제를 설명하여라.

‘Arp cache poisoning’은 네트워크 보안 공격 기술 중 하나로, 이를 통해 공격자는 네트워크 트래픽을 조작하고 중간자 공격(man-in-the-middle)을 수행할 수 있다. ARP(Address Resolution Protocol)은 IP주소를 해당하는 MAC 주소로 매핑하기 위해 사용되는 프로토콜이다. ARP 캐시에는 IP 주소와 해당하는 MAC 주소 간의 매핑 정보가 저장된다. ARP cache poisoning 공격은 이 ARP 캐시를 조작하여 트래픽을 다른 곳으로 리디렉션할 수 있다.

텍스트이(가) 표시된 사진

자동 생성된 설명

그림 8. ARP cache poisoning 공격 캡처 화면

만약 공격자가 ARP cache poisoning 공격을 성공적으로 수행했다면, 다음과 같은 정보를 확인할 수 있다. ARP 테이블을 확인하면, 정상적인 IP주소와 해당하는 MAC 주소 간의 매핑을 확인 및 변조되어 있을 수 있다. 공격자가 공격을 통해 목표로 하는 트래픽을 중간에 가로챌 수 있도록 피해자의 IP주소에 대한 MAC 주소를 공격자의 MAC 주소로 변경하는 것이 대부분이다. 따라서 IP주소 101, 111, 254가 동일한 물리주소 b8:ac:6f:de:2c:e1의 MAC주소로 변경된 것을 확인할 수 있다.

3. 아래 그림에서 볼 수 있듯이 새로운 보안 담당자에게 사용되지 않는 스위치의 포트에서 네트워크 캡처를 설정하도록 요청하였다. 활성화된 네트워크 상에서 몇 시간의 캡처를 한 후에 확인해보니, 캡처된 모든 것이 브로드캐스트 트래픽이었다. 무엇이 문제인가?

테이블이(가) 표시된 사진

자동 생성된 설명

그림 9. 브로드캐스트 트래픽

스위치는 일반적으로 스위치 포트에서 전송된 패킷을 해당 포트의 연결된 장치의 MAC 주소를 통해 정확하게 전달된다. 따라서 네트워크의 브로드캐스트 패킷은 모든 장치에 전송되기 때문에, 스위치의 포트가 확장되지 않은 경우 해당 포트를 통해서 수신된 모든 패킷이 브로드캐스트 패킷이 될 가능성으로 짐작할 수 있었다.

* 1. 실습 2: Wireshark 를 이용한 패킷 분석

1. 패킷 분석을 위해 FTP 서버([ftp.kaist.ac.kr](ftp://ftp.kaist.ac.kr))에 접속하여 로그인을 한다.

(USER: anonymous, PASS: 1234)

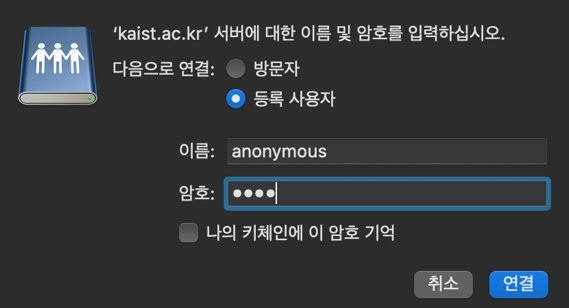


그림 10. FTP(fpt.kaist.ac.kr) 접속

FTP는 “File Transfer Protocol”로, 컴퓨터 네트워크를 통해 파일을 전송하기 위해 사용되는 프로토콜이다. FPT는 client-server 모델을 기반으로 작동하며, 클라이언트는 파일을 업로드하거나 다운로드하기 위해서, 서버는 클라이언트 요청을 처리하고 파일을 관리하기 위해 해당 소프트웨어를 사용하게 된다. 또한 이번 실습에서 확인하고자 하는 사용자 인증도 제공한다.

이외의 기능으로 ‘디렉토리 및 파일 관리’, ‘포트 및 데이터 전송 모드’, ‘보안’과 같은 기능을 제공한다.

2. 패킷 캡처를 중지하고 String 검색을 통해 USER와 PASS를 검색하여 패킷을 확인한다.

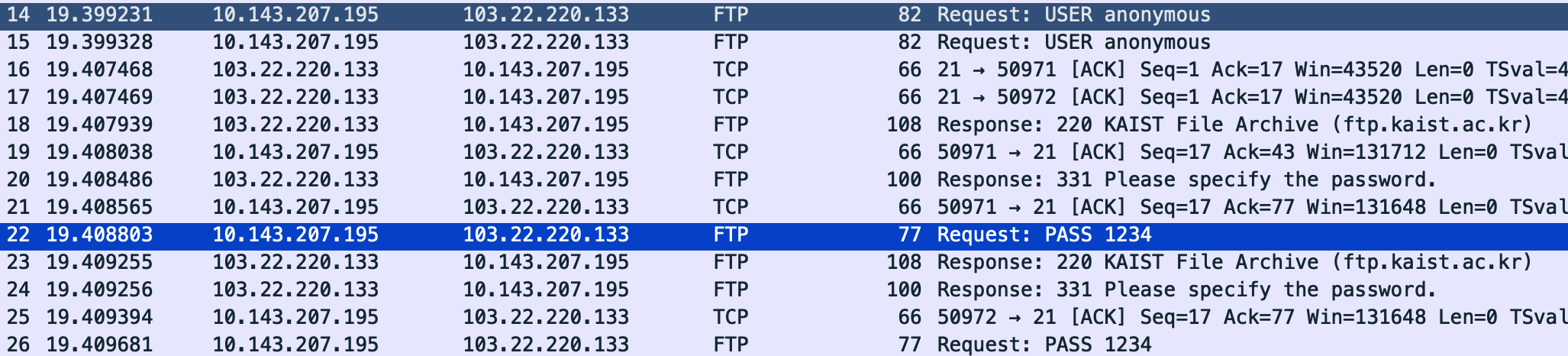


그림 11. USER와 PASS 정보가 담긴 패킷 확인

그림 10과 같이 FTP 서버에 USER와 PASS 정보를 통한 사용자 인증을 위한 패킷 전송을 했을 때, 해당 패킷이 캡처되어 있음을 확인할 수 있다. 입력 데이터 그대로 USER에는 anonymous, PASS에는 1234가 전송된 것을 확인할 수 있다. 이를 통해 사용자 인증 기능에서 보안이 되지 않는 점을 알 수 있다.

3. FTP에 접속한 USER와 PASS를 너무나 쉽게 확인할 수 있다. 이를 방지하기 위해 어떤 방법을 적용할 수 있는지 기술하시오.

FTP 서버에 로그인할 때 USER와 PASS 정보가 패킷 분석 도구를 통해 평문으로 확인되는취약점이 있어 이를 방지해야 한다.

**FTPS**는 FPT에 보안 계층인 SSL/TLS 를 추가한 프로토콜로 FTPS를 사용하면 클라이언트와 서버 간의 통신이 암호화되어 평문으로 전송되는 것을 방지할 수 있을 수 있다. 이는 패킷이 평문으로 전송되어 확인할 수 있다는 점에서 생각해 볼 수 있다. 또한 **SFTP**를 사용하는 것도 있다. SSH(Secure Shell) 프로토콜을 사용하여 파일 전송을 제공한다. SSH는 암호화된 연결을 제공하여 USER와 PASS 정보가 보호된다. 이외에도 **VPN(Virtual Private Network)**를 구성하여 클라이언트와 서버 간의 통신을 암호화하여 전송할 수 있어 취약점을 해결할 수 있다.

2.4 실습 3: ICMP 패킷 디코딩 수행

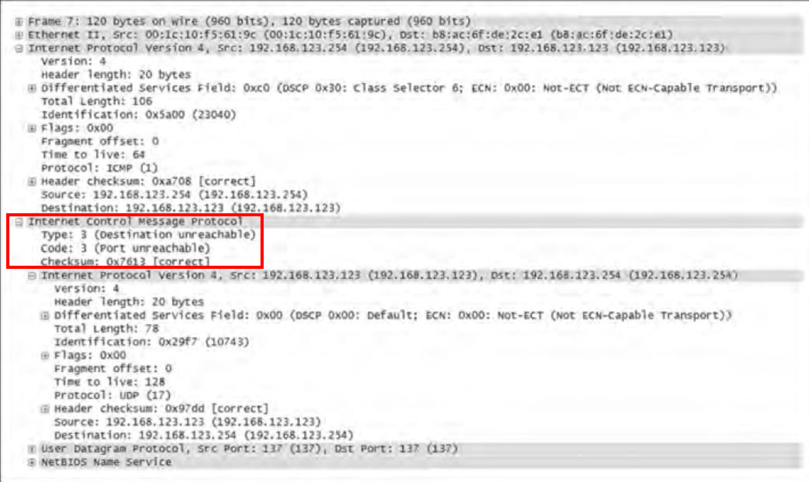


그림 12. ICMP 패킷과 세부사항

ICMP(Internet Control Message Protocol)는 인터넷 프로토콜의 비신뢰적인 특성을 보완하기 위한 프로토콜로 IP 패킷 전송 중 에러 발생 시 에러 발생 원인을 알려주거나 네트워크 상태를 진단해주는 기능을 제공한다. ICMP 메시지의 포맷은 다음 그림 13과 같다.

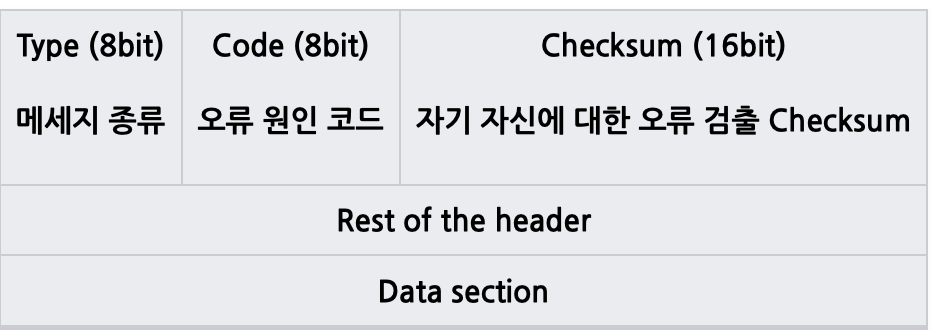


그림 13. ICMP 메시지 포맷

메시지의 종류를 확인해보면 다양한 유형으로 분류할 수 있다. 전송한 패킷이 목적지에 도달하지 않은 경우, 혼잡으로 인한 데이터그램이 drop이 되거나 Timeout, IP 패킷 또는 헤더의 오류, 경로 재지정과 같은 유형으로 분류할 수 있다.

1. 문제가 발견된 호스트의 IP주소는 무엇인가

문제가 발견된 호스트의 IP주소는 Destination 주소로 192.168.123.123으로 호스트로부터 ICMP 메시지를 전송하여 네트워크의 상태를 진단하고자 하는 목적지 주소에 대해서 문제가 발생했음을 알 수 있다.

2. 원래 호스트의 IP주소는 무엇인가

원래 호스트의 IP주소는 192.168.123.254로 ICMP 메시지를 보낸 호스트의 주소임을 알 수 있다.

3. ICMP 유형과 코드 에러는 무엇인가

Type 3 오류는 목적지 호스트나 네트워크로의 패킷 전달 중 발생하는 문제를 알려준다. 해당 Type에서는 code로 다양한 문제를 식별할 수 있으며, 위 문제에서는 Code3로 Port Unreachable이다. 해당 문제는 송신 호스트가 목적지 호스트의 특정 포트에 도달할 수 없음을 나타낸다. 일반적으로 목적지 호스트에서 해당 포트에 대해서 활성화되지 않았거나, 방화벽이 해당 포트를 차단하는 경우에 발생하게 된다.

이외에 Type3의 에러 Code는 다음과 같다.  
 code 0 (Network Unreachable) : 송신 호스트가 목적지 네트워크에 도달할 수 없어 라우팅 문제로 예상할 수 있다.

code 1(Host Unreachable): 목적지 호스트가 다운되었거나 네트워크에 접근할 수 없는 상태일 때 발생할 수 있다.

code 2(Protocol Unreachable): 송신 호스트가 패킷을 전달하려는 프로토콜이 목적지 호스트에서 지원되지 않는 경우가 있을 수 있다.

4. 송신 장치는 어느 포트를 가지고 통신을 시도하는가

User Datagram Protocol의 SPC Port를 확인하면 137번인 것을 확인할 수 있다. NETBOIS-NS(NETBIOS Name Service)로 이름 등록과 관련한 포트 번호이다.

5. 구체적인 문제는 무엇인가

해당 오류는 송신 호스트가 패킷을 특정 목적지 호스트의 특정 포트로 전달할 수 없음을 나타낸다. 특히 포트번호가 137로 송신 장치의 포트가 명시된 점을 통해 네트워크에 NetBIOS 이름을 등록해 네트워크에 통신하고자 하는 패킷을 전송했지만 해당 포트에 도달하지 못한다는 문제를 짐작할 수 있다.

2.5 실습 4: Trace Route

1. [www.rutgers.edu](http://www.rutgers.edu)의 경로를 찾기 위해 Traceroute 사용

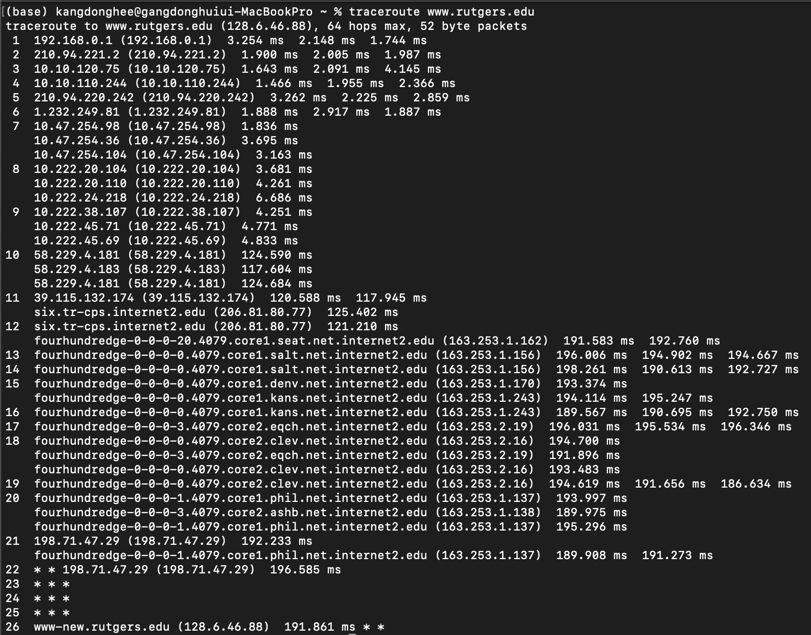


그림 14. 주어진 DNS의 경로 추적

2. Traceroute 결과에서 보이는 것은 어떤 종류의 정보인가?

(1) 중간 라우터의 IP주소

(2) 응답시간 : 각 라우터에 전송한 패킷의 응답 시간을 확인할 수 있다.

(3) 패킷 손실: 각 라우터로 전송한 패킷이 도달하는지 여부를 확인한다.

(4) TTL: TTL 값을 조정하여 라우터의 수를 추적할 수 있다.

3. 와이어샤크를 사용해 IP 헤더에 있는 TTL을 관찰하라. 왜 3 패킷마다 증가하는가?

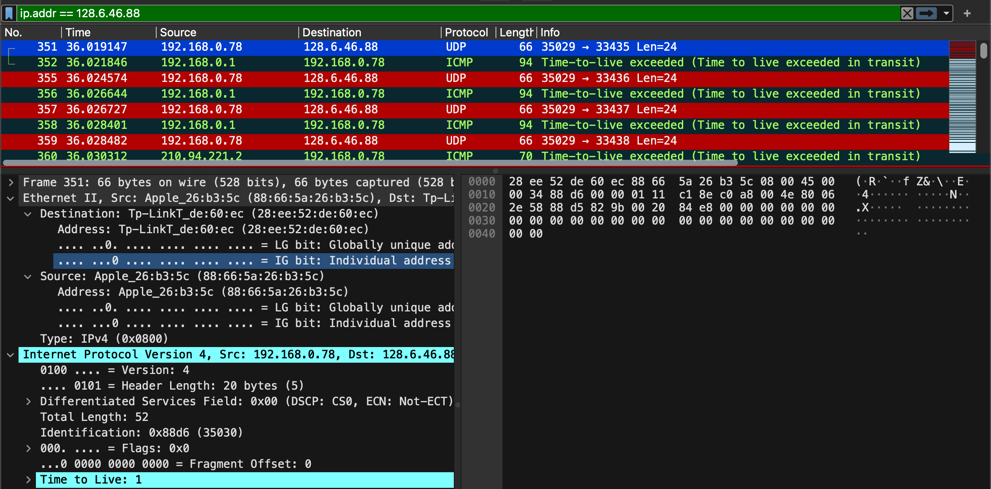


그림 15. 그림 14의 실행 중 와이어샤크 캡처 결과

TTL 값은 네트워크 상에서 패킷이 무한 루프를 돌지 않도록 제한한 값이다. TTL 값은 패킷을 전송하는 동안 각 라우터에서 TTL 값을 1씩 감소시키며, TTL 값이 0이 되면 해당 패킷은 버려지고 에러 메시지가 생성된다.

TTL 값을 3개의 패킷마다 증가시키는 것은 네트워크 상에서 다양한 라우터를 거치게 되는데 이때 TTL 값이 감소하면서 패킷은 라우터를 통과하게 되고, TTL이 0이 되면 버려지게 되는데 TTL 값을 기반으로 패킷이 거치는 경로를 추적하기 위해 3개의 패킷마다 증가시킨다.

1. 공개 Traceroute 서버를 사용해 로컬 경로와 비교해라.

텍스트이(가) 표시된 사진

자동 생성된 설명

그림 16. 공개 서버 Traceroute 결과

공개 Traceroute 서버와 로컬 Traceroute 의 경로는 서로 다른 라우팅 경로를 가질 수 있다. 패킷이 전송되는 경로는 네트워크 환경과 정책에 따라 다를 수 있어 경로가 서로 다를 수 있게 된다. 또한 공개 Traceroute 서버는 지리적으로 다른 위치에 있어 인터넷의 물리적 구조와 서버의 위치에 따라 경로가 다를 수 있게 된다.

5. 다음 예에서 장비의 종류와 포트, 또는 홉마다 가진 다른 속성을 확인할 수 있는가?

Traceroute를 통해 ICMP 응답을 분석하여 각 홉의 지연시간을 측정하고, 해당 Ip주소에 대한 정보를 알아낼 수 있지만, 구체적인 정보를 확인하기에는 어렵다.

6. 동일한 예를 사용하여 마지막 라인들이 왜 공백이며 일반적으로 Traceroute가 목적지에 도달했는지 여부를 어떻게 알려주는가?

Traceroute가 목적지에 도달한 여부는 마지막 응답에 최종 주소와 평균 응답 시간 및 지연 시간의 전송 결과를 통해서 확인할 수 있다. 또한 마지막 라인이 공백을 통해 경로 추적이 완료되었음을 알 수 있게 된다.

3 결 론

3.1 느낀 점

이번 실습을 통해 주로 ICMP(Internet Control Message Protocol)에 대해 다양한 실습과 이론을 배울 수 있었다. 와이어샤크 오픈소스 프로그램을 통해 컴퓨터와 통신하는 모든 패킷을 분석하여 나의 네트워크 상태를 점검할 수 있다는 점에서 다양하게 활용할 수 있을 것 같다. 또한 보안 이론 수업에서 배운 다양한 이론들도 직접 확인할 수 있었다. 특히, ICMP를 통해 네트워크의 통신 상태를 점검하는 부분에서 다양한 타입과 코드에 따라서 점검 및 해결할 수 있는 부분을 확인할 수 있다. 실생활에서도 발생하는 다양한 네트워크 문제도 이를 통해서 해결할 수 있다는 것을 알 수 있었으며, 취약점에 대해서도 고민할 수 있게 되었다. 따라서 인터넷과 통신을 하면서 발생하는 다양한 동작 과정과 위험, 취약점에 대해서 알 수 있었다.