컴퓨터 보안_01

실습 9주차

동국대학교 CSDC Lab.
실습조교 김선규, 최연우
2022.04.13 (Wed.)

Index

Wireshark introduce

dongguk UNIVERSITY

➢ 와이어샤크(Wireshark)

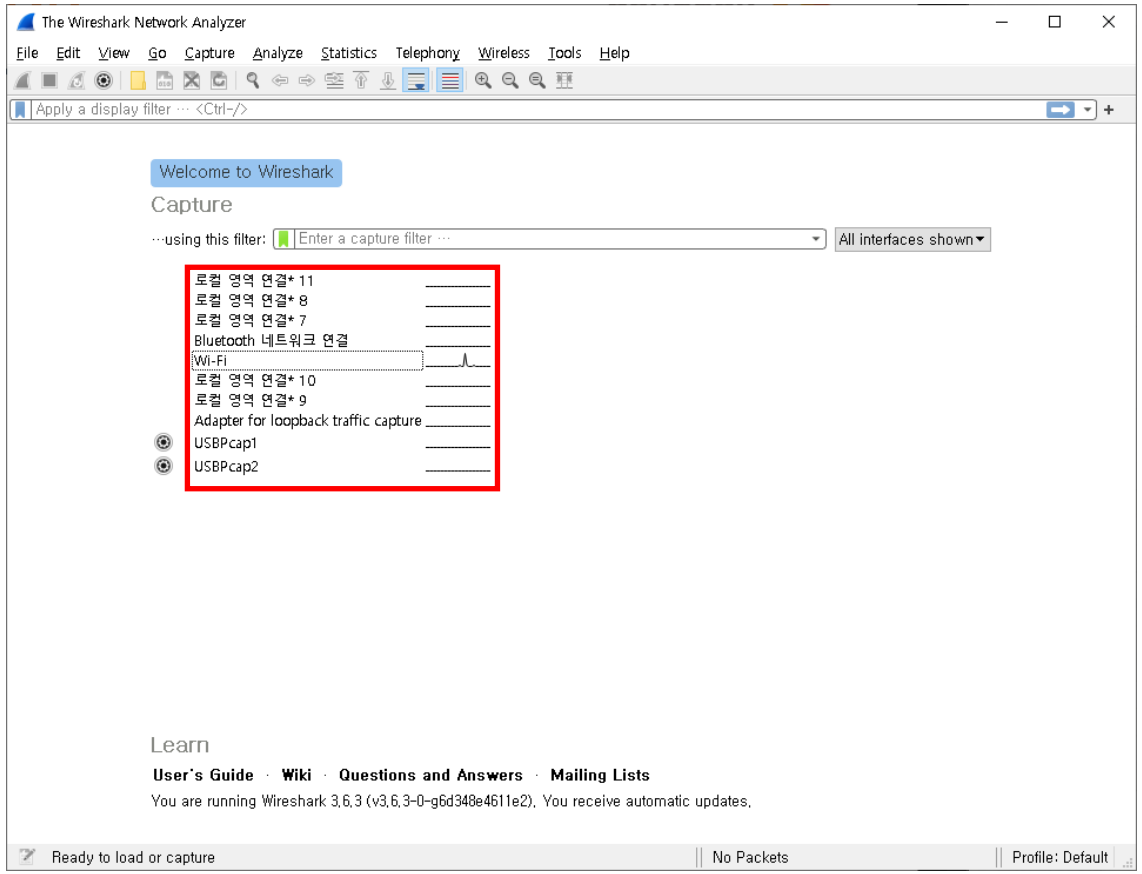
- 와이어샤크는 자유 및 오픈 소스 패킷 분석 프로그램이며 네트워크의 문제, 분석, 소프트웨어 및 통신 프로토콜 개발, 교육에 쓰인다.
- 원래 이름은 Ethereal이었지만 상표 문제로 와이어샤크(Wireshark)로 바꾸게 되었다.
- Libpcap 형식으로 확장자는 “pcap”을 사용하며 패킷을 잡아내는 것이 주요 기능이다.
- “통신망의 상어 " 라는 뜻을 지니고 있으며 이름이 컨셉 그 자체이다.
- 실시간 네트워크 연결의 유선으로부터 데이터를 포획하고, 이미 포획한 패킷을 기록해둔 파일로부터 데이터를 읽을 수 있다.
- 실시간 데이터를 이더넷, IEEE 802.11, PPP, 루프백을 포함한 수많은 네트워크로부터 읽을 수 있다.
- 포획한 네트워크 데이터는 GUI나 터미널 (명령 줄) 버전의 유틸리티 TShark를 통해 탐색할 수 있다.

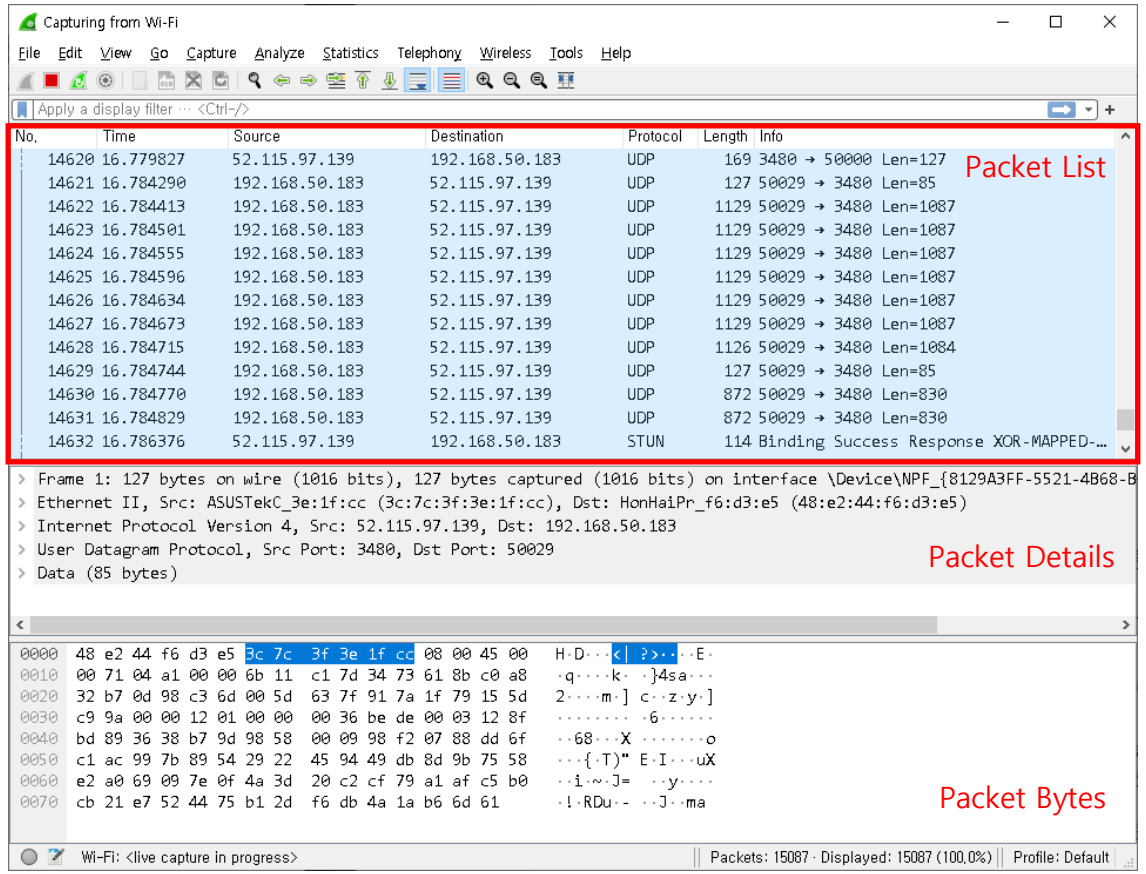
➢ Wireshark Windows Installer

- https://www.wireshark.org/download.html
- 본인의 운영체제에 맞는 64/32-bit Windows Installer 다운로드 후 설치하면 된다.
- Stable Release 버전을 권장하며 2023년 5월 3일 기준 Stable 버전은 4.0.5 버전이다.

➢ 와이어샤크 가이드(Wireshark Guide)

- 와이어샤크 설치 후 좌측 화면을 바로 확인 가능하며 Wi-Fi 부분을 살펴보면 그래프가 그려지고 있다. (본인 네트워크 확인 후 더블 클릭)
- 우측 사진은 와이어샤크 인터페이스 모습이다. No, Time, Source(송신지), Destination(수신지), Protocol, Length, info …

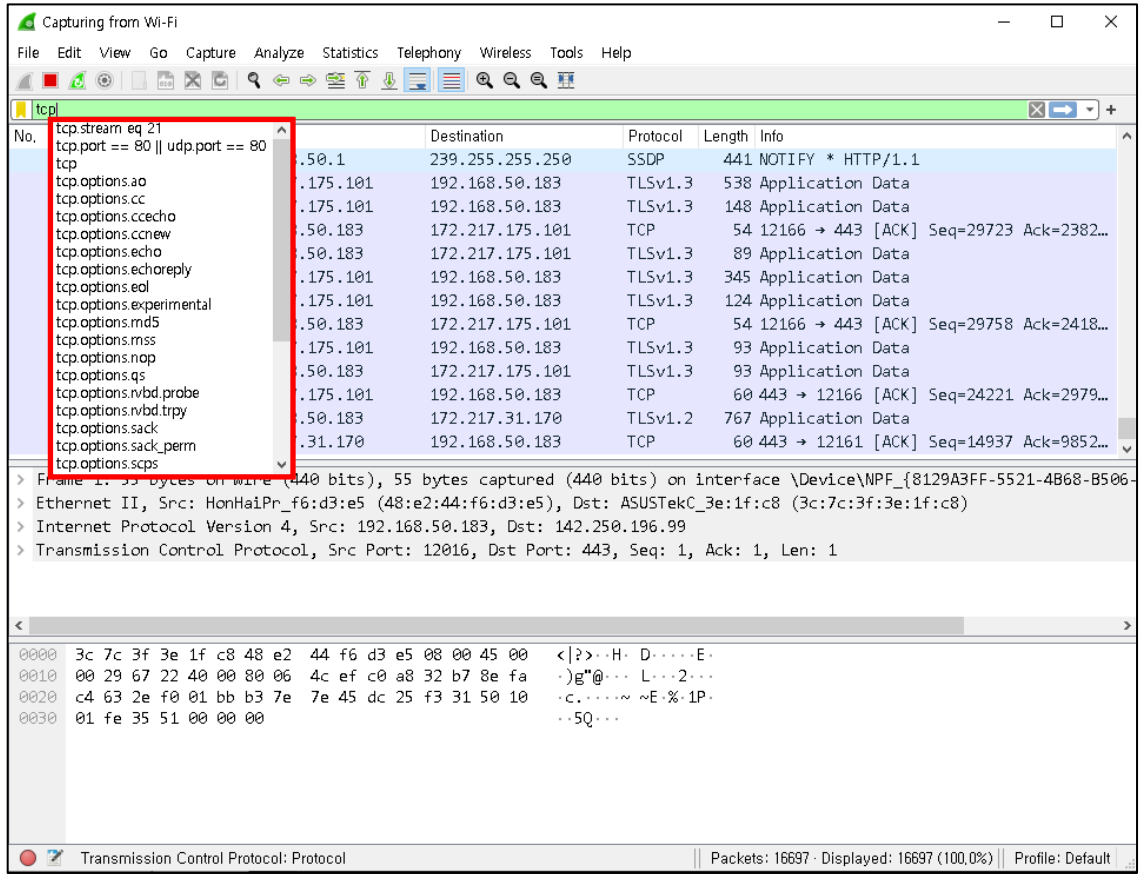


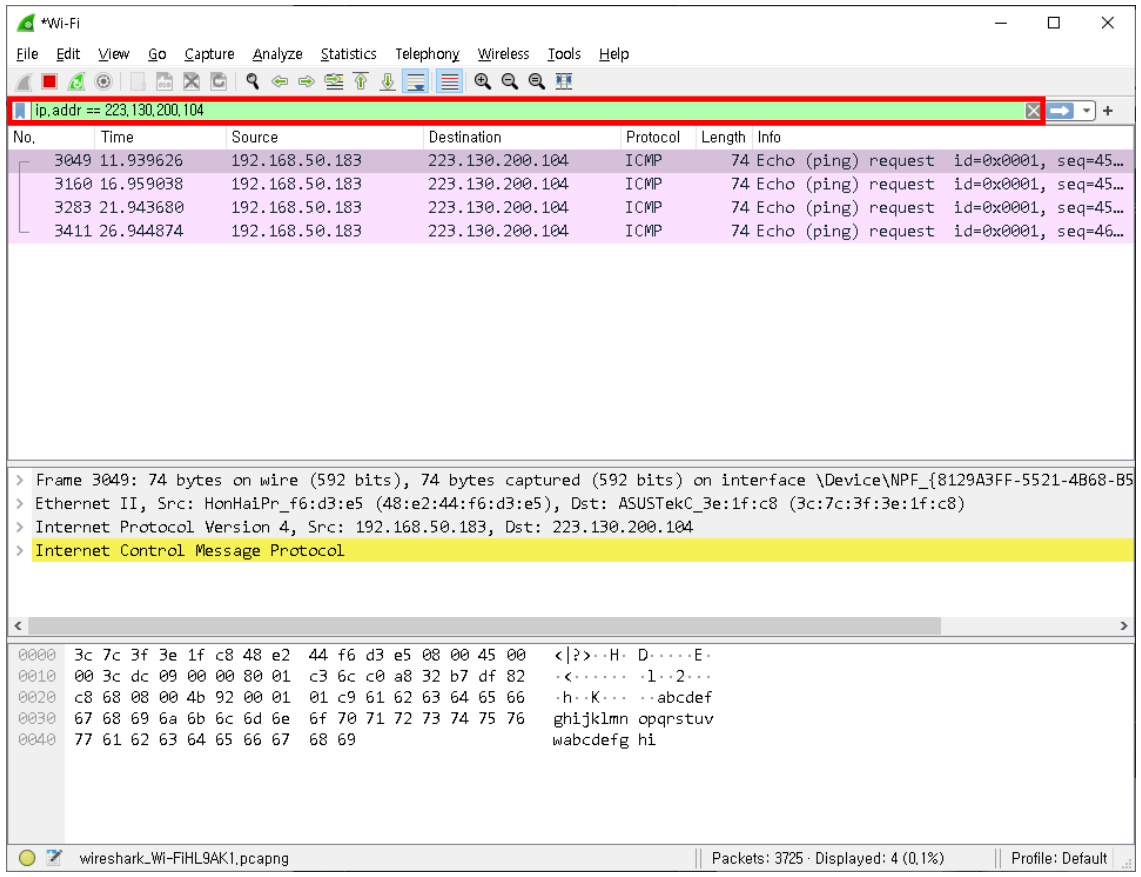


Wireshark Filter

➢ 와이어샤크 필터(Wireshark Filter)

- 다음은 필터를 사용하는 방법 중 하나이다. 우측 사진은 네이버 아이피(223.130.200.104)를 필터링하고 패킷을 확인한 모습이다.
- Filtering while capturing : https://www.wireshark.org/docs/wsug_html_chunked/ChCapCaptureFilterSection.html

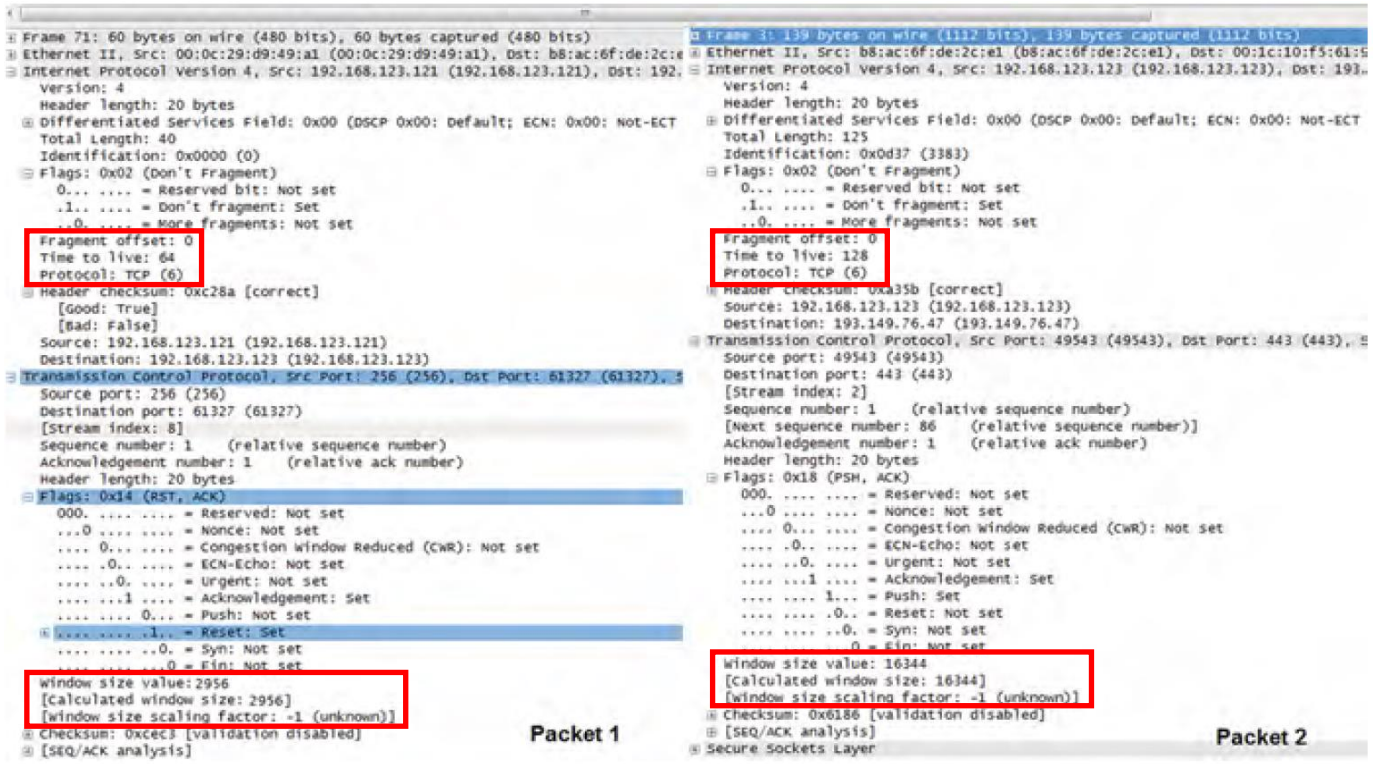




실습#6-1: 패킷 가지고 놀기 (Fun with Packets)

➢ 아래의 각 실습에 대한 수행 결과를 캡처하여 분석하고 설명하는 내용을 개인적인 견해와 함께 레포트에 모두 반영하여야 한다.

1. 아래 그림을 조사해보고 packet1과 packet2의 운영체제가 무엇인지 추측 해보시오.



- 검토해야할 몇가지 항목에는 TTL(Time to Live), 단편화(fragment) 안함, 윈도우 크기가 포함된다.

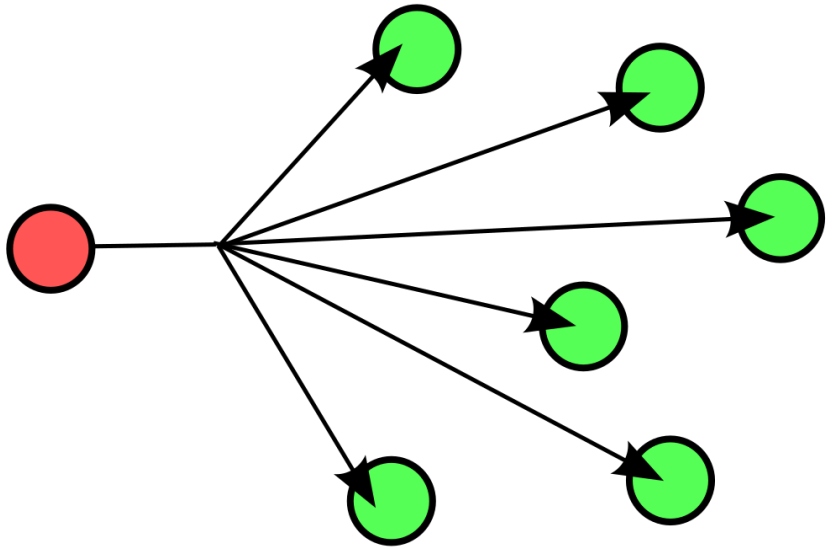
실습#6-1: 패킷 가지고 놀기 (Fun with Packets)

dongguk UNIVERSITY

2. 아래의 그림을 조사해보고 보안 문제를 설명하여라.

564	40.669743	b8:ac:6f:de:2c:e1	10:9a:dd:ab:87:d2	ARP	42 who has 192.168.123.114? Tell 192.168.123.254
565	40.669792	00:80:77:df:b9:ab	b8:ac:6f:de:2c:e1	ARP	60 192.168.123.118 is at 00:80:77:df:b9:ab
566	40.669891	b8:ac:6f:de:2c:e1	00:1c:10:f5:61:9c	ARP	42 192.168.123.253 is at b8:ac:6f:de:2c:e1
567	40.669905	00:1c:10:f5:61:9c	b8:ac:6f:de:2c:e1	ARP	60 192.168.123.254 is at 00:1c:10:f5:61:9c
568	40.670026	b8:ac:6f:de:2c:e1	00:24:a5:d7:90:46	ARP	42 192.168.123.254 is at b8:ac:6f:de:2c:e1
569	40.670061	00:1c:10:f5:61:9c	b8:ac:6f:de:2c:e1	ARP	60 192.168.123.254 is at 00:1c:10:f5:61:9c
570	40.670231	00:e0:11:05:fd:53	b8:ac:6f:de:2c:e1	ARP	60 192.168.123.111 is at 00:e0:11:05:fd:53
571	40.670341	00:1c:10:f5:61:9c	b8:ac:6f:de:2c:e1	ARP	60 192.168.123.254 is at 00:1c:10:f5:61:9c
572	40.670564	00:1c:10:f5:61:9c	b8:ac:6f:de:2c:e1	ARP	60 192.168.123.254 is at 00:1c:10:f5:61:9c
573	40.670779	00:1c:10:f5:61:9c	b8:ac:6f:de:2c:e1	ARP	60 192.168.123.254 is at 00:1c:10:f5:61:9c
574	40.677368	b8:ac:6f:de:2c:e1	00:1c:10:f5:61:9c	ARP	42 192.168.123.110 is at b8:ac:6f:de:2c:e1
575	40.677431	b8:ac:6f:de:2c:e1	6c:33:a9:11:33:0c	ARP	42 192.168.123.254 is at b8:ac:6f:de:2c:e1
576	40.678290	00:22:58:1d:ac:27	b8:ac:6f:de:2c:e1	ARP	60 192.168.123.101 is at 00:22:58:1d:ac:27
577	40.684366	b8:ac:6f:de:2c:e1	00:1c:10:f5:61:9c	ARP	42 192.168.123.111 is at b8:ac:6f:de:2c:e1
578	40.684490	b8:ac:6f:de:2c:e1	00:e0:11:05:fd:53	ARP	42 192.168.123.254 is at b8:ac:6f:de:2c:e1
579	40.691232	b8:ac:6f:de:2c:e1	00:1c:10:f5:61:9c	ARP	42 192.168.123.101 is at b8:ac:6f:de:2c:e1
580	40.691289	b8:ac:6f:de:2c:e1	00:22:58:1d:ac:27	ARP	42 192.168.123.254 is at b8:ac:6f:de:2c:e1
581	40.697739	b8:ac:6f:de:2c:e1	00:1c:10:f5:61:9c	ARP	42 192.168.123.116 is at b8:ac:6f:de:2c:e1
582	40.697795	b8:ac:6f:de:2c:e1	78:45:c4:1e:2f:1f	ARP	42 192.168.123.254 is at b8:ac:6f:de:2c:e1
583	40.704283	b8:ac:6f:de:2c:e1	00:1c:10:f5:61:9c	ARP	42 192.168.123.118 is at b8:ac:6f:de:2c:e1

- 이것은 ARP 캐쉬 포이즈닝(cache poisoning) 공격을 캡쳐한 것이다.
- ARP 캐쉬 포이즈닝 기법과 원리에 대해 조사하고, IP 주소 101 과 111, 그리고 254 모두가 어떻게 같은 물리 주소인 b8:ac:6f:de:2c:e1 을 가질 수 있게 되었는지 추측하여 발생할 수 있는 문제점에 대해 설명하시오.
-



실습#6-1: 패킷 가지고 놀기 (Fun with Packets)

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

Source	Destination
78:45:c4:1e:2f:1f	ff:ff:ff:ff:ff:ff
78:45:c4:1e:2f:1f	ff:ff:ff:ff:ff:ff
10:9a:dd:ab:87:d2	ff:ff:ff:ff:ff:ff
10:9a:dd:ab:87:d2	ff:ff:ff:ff:ff:ff
10:9a:dd:ab:87:d2	ff:ff:ff:ff:ff:ff
10:9a:dd:ab:87:d2	ff:ff:ff:ff:ff:ff
10:9a:dd:ab:87:d2	ff:ff:ff:ff:ff:ff
10:9a:dd:ab:87:d2	ff:ff:ff:ff:ff:ff
10:9a:dd:ab:87:d2	ff:ff:ff:ff:ff:ff
10:9a:dd:ab:87:d2	ff:ff:ff:ff:ff:ff
10:9a:dd:ab:87:d2	ff:ff:ff:ff:ff:ff
78:45:c4:1e:2f:1f	ff:ff:ff:ff:ff:ff
78:45:c4:1e:2f:1f	ff:ff:ff:ff:ff:ff
78:45:c4:1e:2f:1f	ff:ff:ff:ff:ff:ff
78:45:c4:1e:2f:1f	ff:ff:ff:ff:ff:ff
78:45:c4:1e:2f:1f	ff:ff:ff:ff:ff:ff
78:45:c4:1e:2f:1f	ff:ff:ff:ff:ff:ff
78:45:c4:1e:2f:1f	ff:ff:ff:ff:ff:ff
78:45:c4:1e:2f:1f	ff:ff:ff:ff:ff:ff
78:45:c4:1e:2f:1f	ff:ff:ff:ff:ff:ff
78:45:c4:1e:2f:1f	ff:ff:ff:ff:ff:ff

- 포트가 확장(spanned)되지 않았다고 답했다면 정답이다.
- 포트가 확장되지 않은 패킷은 브로드캐스트 패킷만 보낼 수 있다.
- 스위치의 역할과 통신 방법에 대해 조사하여 문제에 대한 보충 설명을 기재하시오.

실습#6-2: Wireshark 를 이용한 패킷 분석

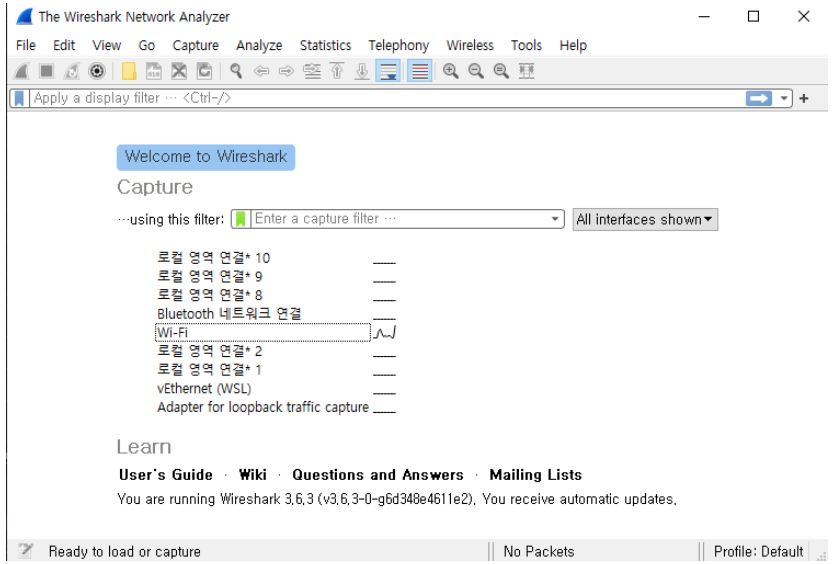
dongguk UNIVERSITY

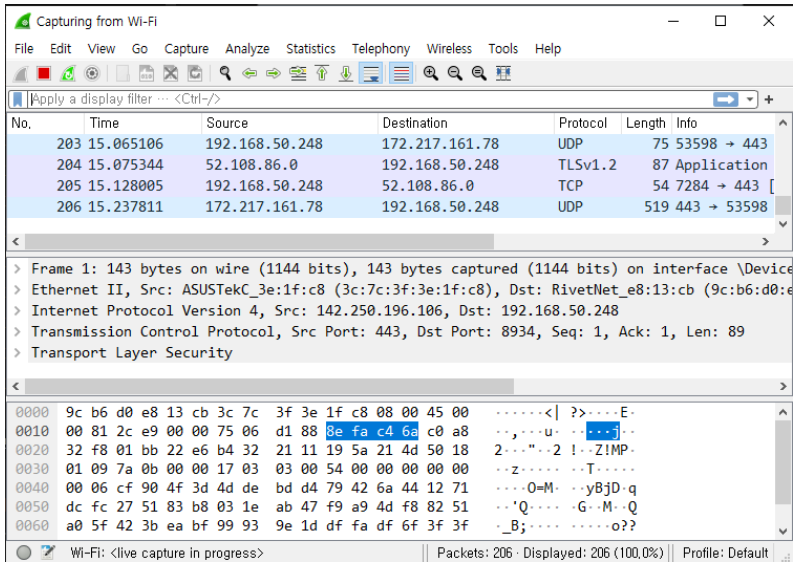
➢ **본 실습에서는 Wireshark를 이용해 어떻게 트래픽을 캡처할 수 있는지를 확인할 수 있다. 이 프로그램은 와이어샤크 공식 홈 페이지에서 다운로드 받을 수 있다.**

1. 윈도우 상에서 Wireshark를 설치하고 트래픽을 캡처하여 실습을 진행한다.

2. 본 실습에서는 Wireshark 상에서 FTP 사용자 이름(USER)과 패스워드(PASS)를 확인할 수 있어야한다.

3. 먼저 Wireshark를 실행하여 본인이 사용하는 네트워크를 선택하면 해당 네트워크 대역에서 통신중인 패킷을 볼 수 있다.

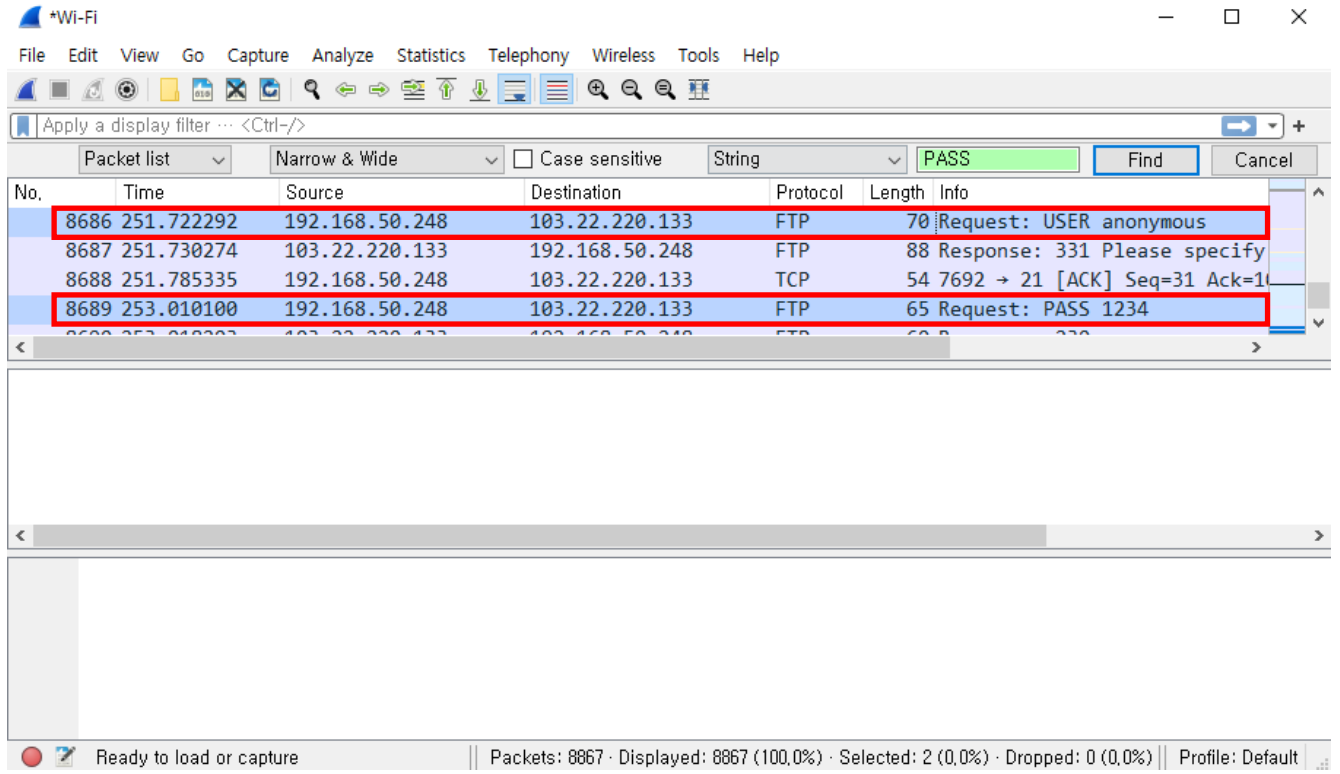




실습#6-2: Wireshark 를 이용한 패킷 분석

4. 이후 명령프롬프트(cmd) 를 실행하여 FTP 접속의 한 예로 KAIST FTP에 접속한다. 접속 방법은 'ftp ftp.kaist.ac.kr' 를 입력하여 KAIST FTP에 접속하고 사용자 이름(USER) : anonymous, 패스워드(PASS) : 1234 를 입력한다.

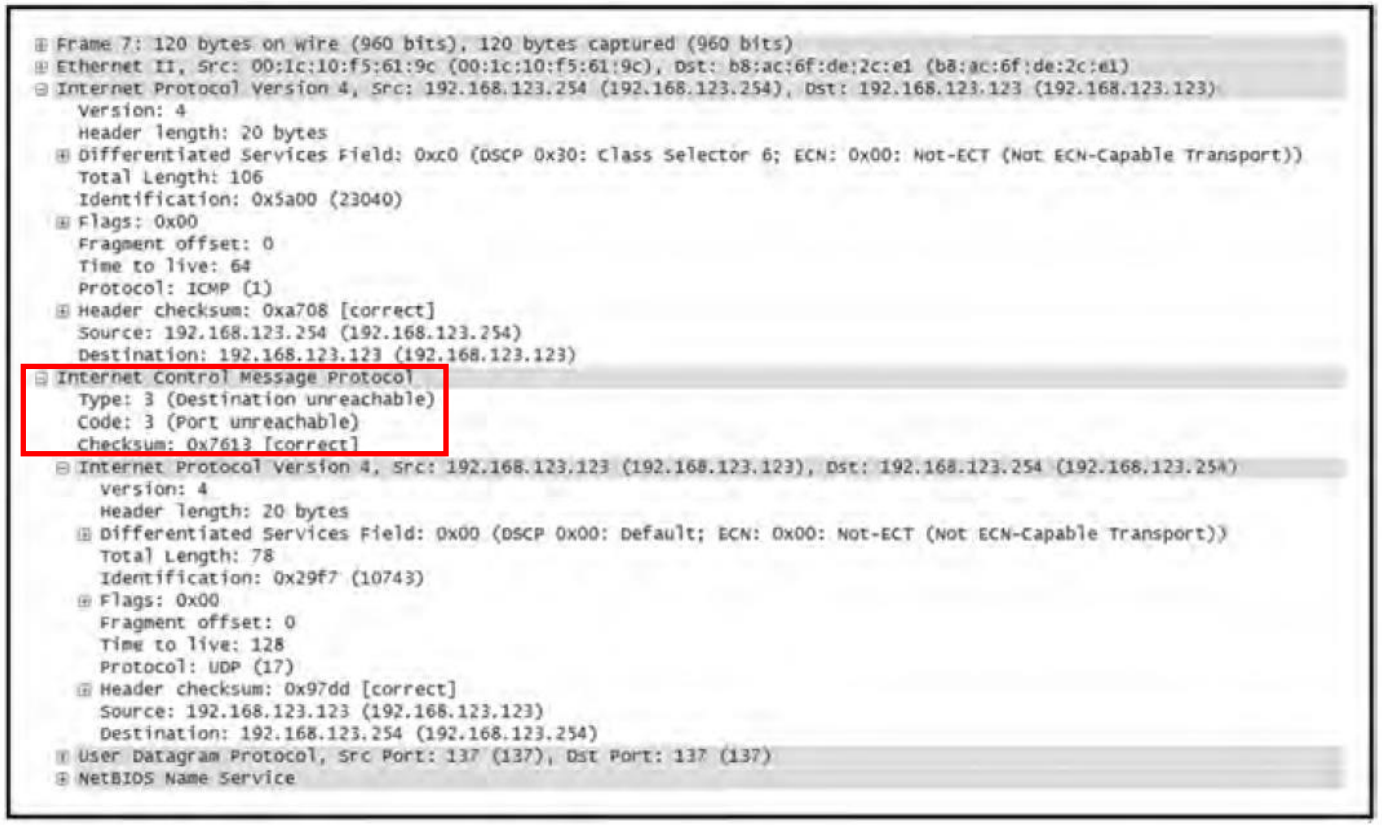
5. 패킷 캡처를 중지하고 String 검색을 통해 USER와 PASS를 검색하여 내가 입력한 USER와 PASS를 입력한 패킷을 확인할 수 있는지 알아보자.



6. FTP에 접속한 USER와 PASS를 너무나 쉽게 확인할 수 있음을 알아보았다. 이를 방지하기 위해서 어떤 방법을 적용할 수 있는지 기술하시오.

실습#6-3: ICMP 패킷 디코딩 수행 (ICMP Packet Decode)

➢ ICMP는 논리적인 에러와 진단을 위해 사용된다. 이 실습은 ICMP에러 메시지를 디코딩하는데 도움이 된다. 아래 그림은 ICMP패킷과 세부사항을 보여준다. 이 그림을 이용하여 다음 질문에 답하여라.



[실습 내용]

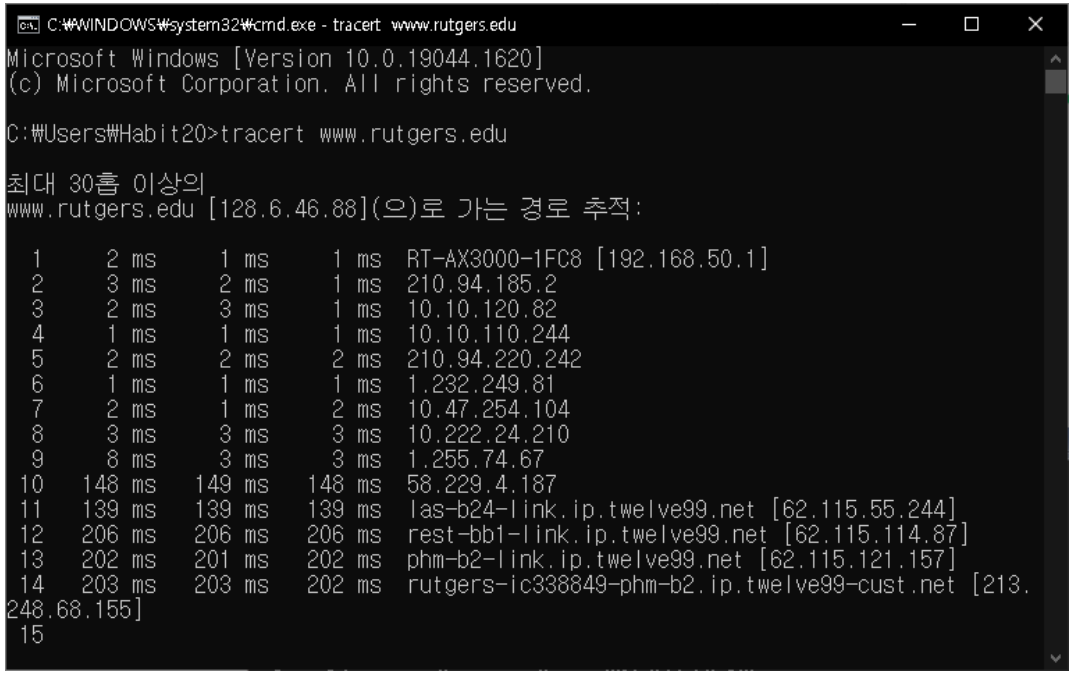
1. 문제가 발견된 호스트의 IP주소는 무엇인가?
2. 원래 호스트의 IP주소는 무엇인가?
3. ICMP유형과 코드 에러는 무엇인가?
4. 송신 장치는 어느 포트를 가지고 통신을 시도하고 있는가?
5. 구체적인 문제는 무엇인가?

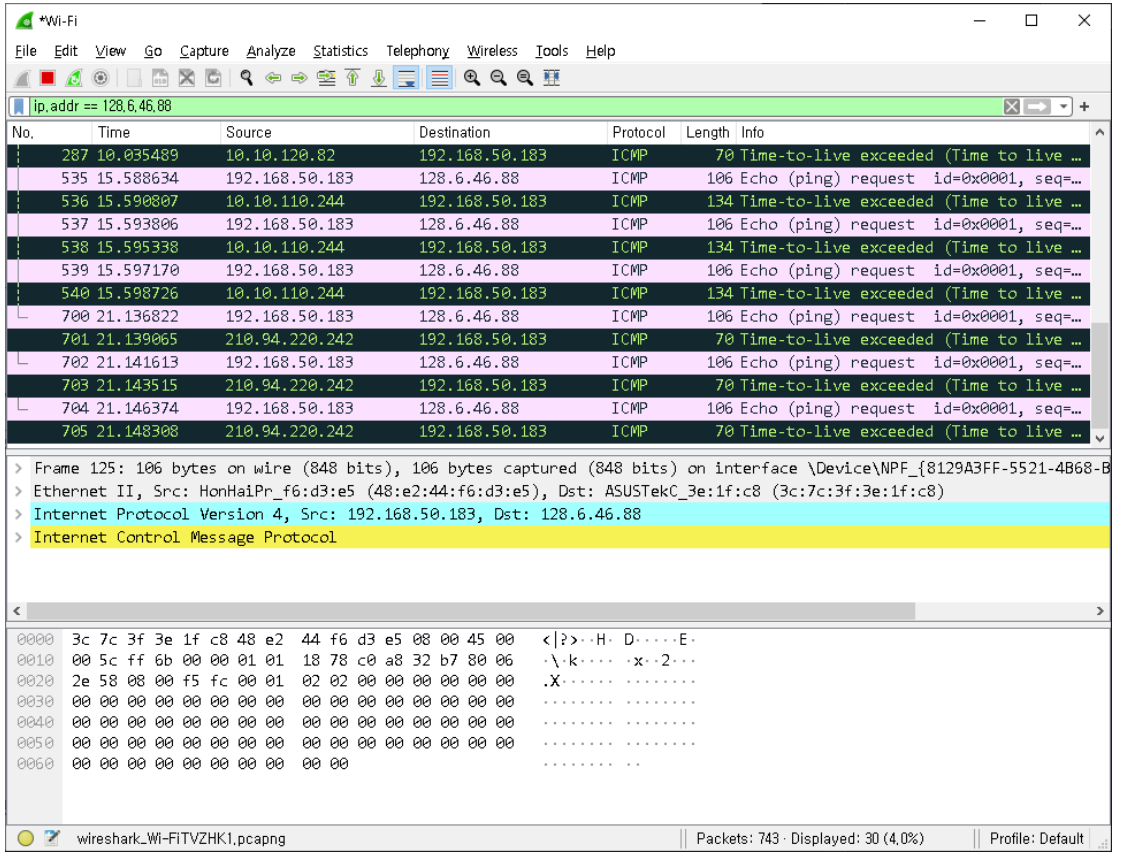
실습#6-4: 트레이스 라우트 (Trace Route)

➢ **이번 실습은 Traceroute가 어떻게 동작하는지를 보여준다.**

Traceroute: 목적하는 서버에 이르기까지 어떤 라우터를 통해 도착하는지를 조사하는 명령

1. www.rutgers.edu로 향하는 경로를 찾기 위해 Traceroute를 사용한다. 이 Traceroute가 실행되는 동안 와이어샤크를 사용하는 것이 좋다.





실습#6-4: 트레이스 라우트 (Trace Route)

2. Traceroute 결과에서 보이는 것은 어떤 종류의 정보인가?

3. 와이어샤크를 사용해서 IP헤더에 있는 TTL을 관찰하여라. TTL은 3개의 패킷마다 증가한다. 왜 증가하는가?

4. www.traceroute.org(Germany - HanNet 권장)에서 선택한 공개 Traceroute 서버를 사용하여라. 그곳에서 www.rutgers.edu로 Traceroute 를 실행하여라. 로컬 Traceroute 의 경로와 traceroute.org에서 수행한 경로가 같은가? 왜 같거나 다른가?

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

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

실습 과제 및 보고서 진행방법 (1)

dongguk UNIVERSITY

➢ 실습 진행 방법

- 간단한 이론 복습 및 해당주차 실습문제 설명
- 실습 후 보고서를 작성하여 화요일 점심(12:00) 까지 E-Class에 제출(이메일 제출 불가, 반드시 E-Class를 통해 제출)
- 실습 과제 제출 기한 엄수 **(제출기한 이후로는 0점 처리)**

➢ 실습 보고서 [1/2]

- 실습 문제에 대한 요구 사항 파악, 해결 방법 등 기술
- 프로그램 설계 / 알고리즘
  - 해결 방법에 따라 프로그램 설계 및 알고리즘 등 기술
  - 문제 해결 과정 및 핵심 알고리즘 기술
- 결과 / 결과 분석
  - 결과 화면을 캡쳐 하여 첨부, 해당 결과가 도출된 이유와 타당성 분석
- 소감
  - 실습 문제를 통해 습득할 수 있었던 지식, 느낀 점 등을 기술

실습 과제 및 보고서 진행방법 (2)

dongguk UNIVERSITY

➢ 실습 보고서 [2/2]

- 제출 방법
  - 보고서를 작성하여 E-Class “과제” 메뉴를 통해 제출
    - **“이름_학번_실습주차.zip” 형태로 제출 (e.g. : 홍길동_2023123456_실습1주차.zip)**
    - 파일명에 공백, 특수 문자 등 사용 금지
    - 보고서 파일은 한글/워드 등 모두 상관 없지만 **PDF 변환** 후 이클래스 제출 **(압축은 필요한 경우에만 사용)**

- 유의사항
  - 보고서의 표지에는 학과, 학번, 이름, 담당 교수님, 제출일자 반드시 작성
  - 정해진 기한 내 제출
    - **기한을 넘길 시 0점 처리**
    - E-Class가 과제 제출 마지막 날 오류로 동작하지 않을 수 있으므로, 최소 1~2일 전에 제출
    - 당일 E-Class 오류로 인한 미제출은 불인정
  - 보고서를 자신이 작성하지 않은 경우 실습 전체 점수 0점 처리

Q & A