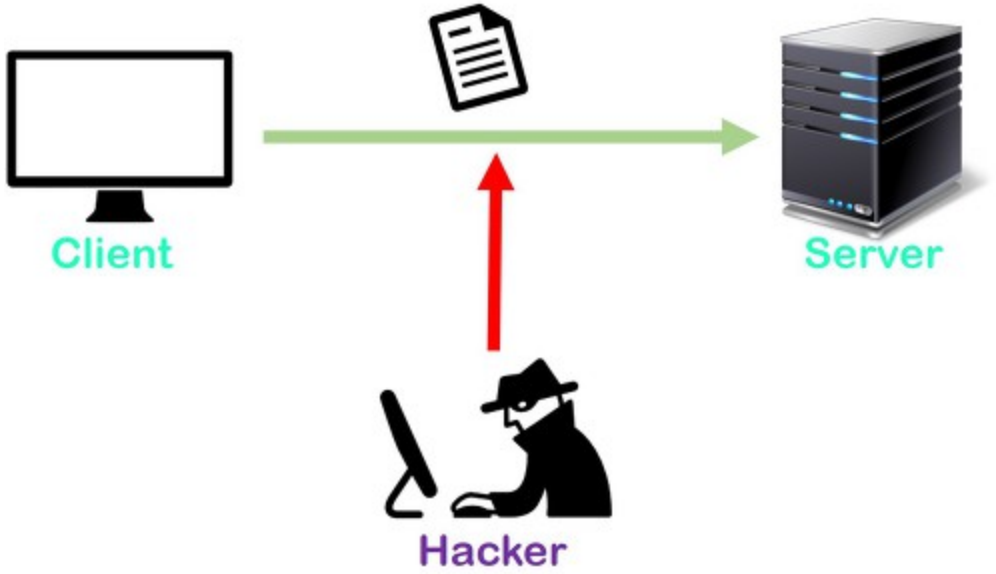
컴퓨터보안 실습

6. 네트워크 보안
(Sniffing 및 패킷 분석)

Sniffing

- **Sniff : 코를 킁킁거리다.**
- 네트워크 상에서 자신이 아닌 다른 사람들의 패킷을 엿보는 행위

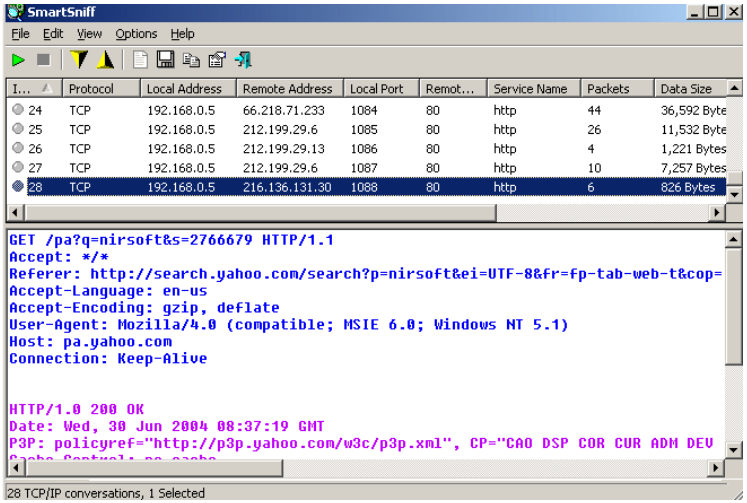


- **즉, 네트워크 트래픽을 도청하는 행위**

Sniffing

- 패킷 분석 및 캡처 프로그램 이용

WireShark

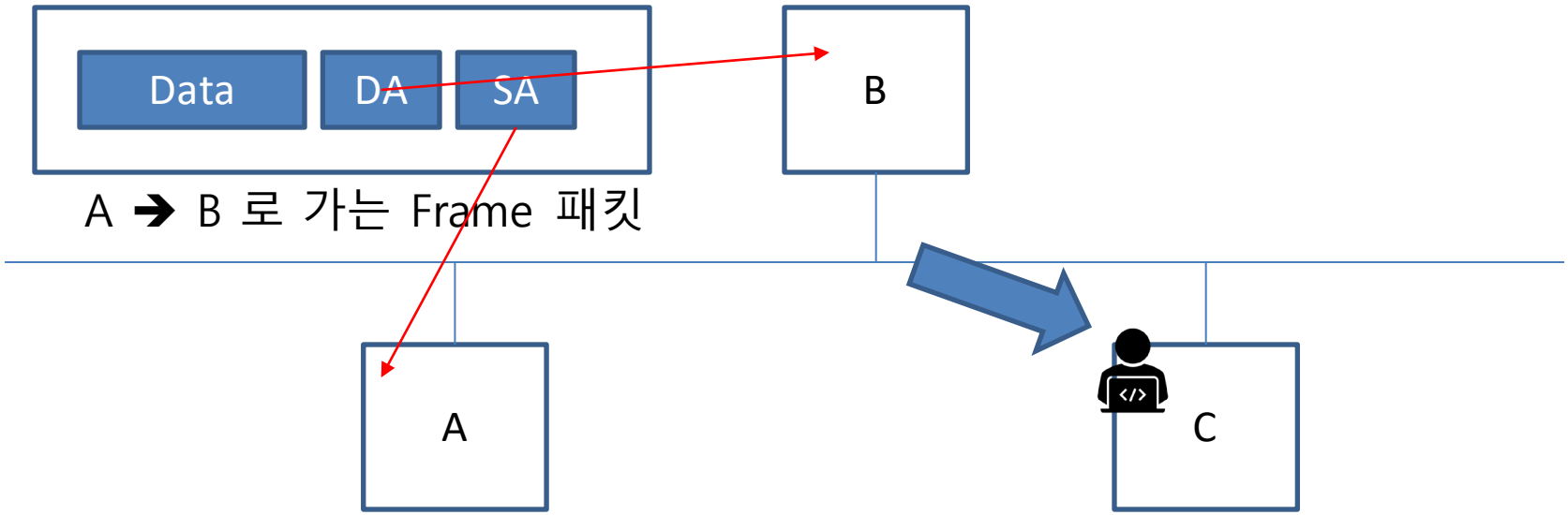


Smart Sniffer

Sniffing

- **프러미스큐어스 (Promiscuous)모드 활성화**

→ 네트워크 상 Lan카드가 패킷을 받을 때, IP주소와 MAC주소가 해당 Lan카드와 다르더라도 패킷을 모두 수집



-논 프러미스큐어스모드 : 자기 자신이 발신인인 패킷 아니면 모두 버림
-프러미스큐어스모드 : 모든 패킷 수용

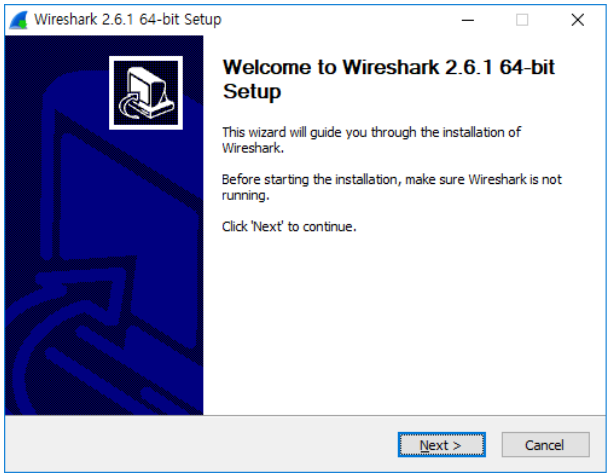
- 리눅스, 유닉스 랜카드 모드변경을 통해 가능
- 윈도우 환경에서는 가상드라이버 설치 후 가능, 제한된 기능

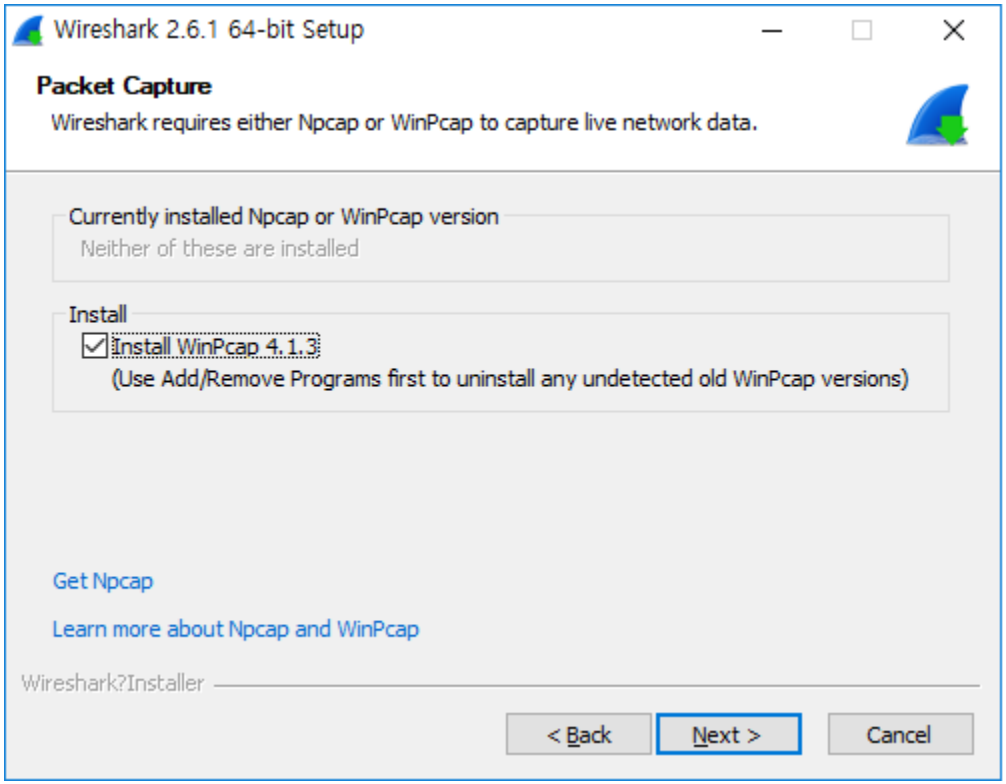
WireShark 설치

- **와이어샤크 다운로드**

→ https://www.wireshark.org/download.html

- **설치 시작**

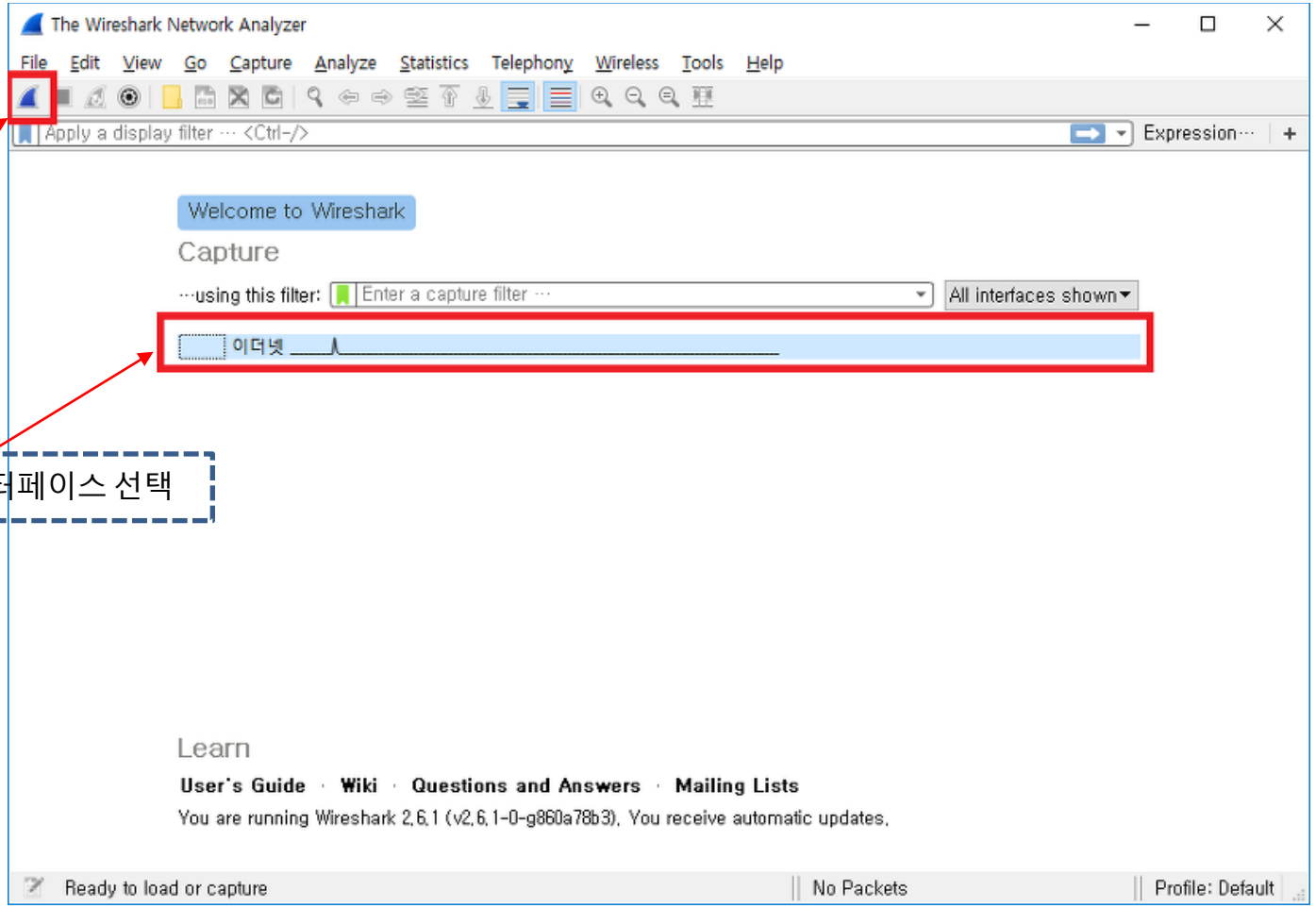




WinPcap은 반드시 설치

WireShark 실행

- **실행**

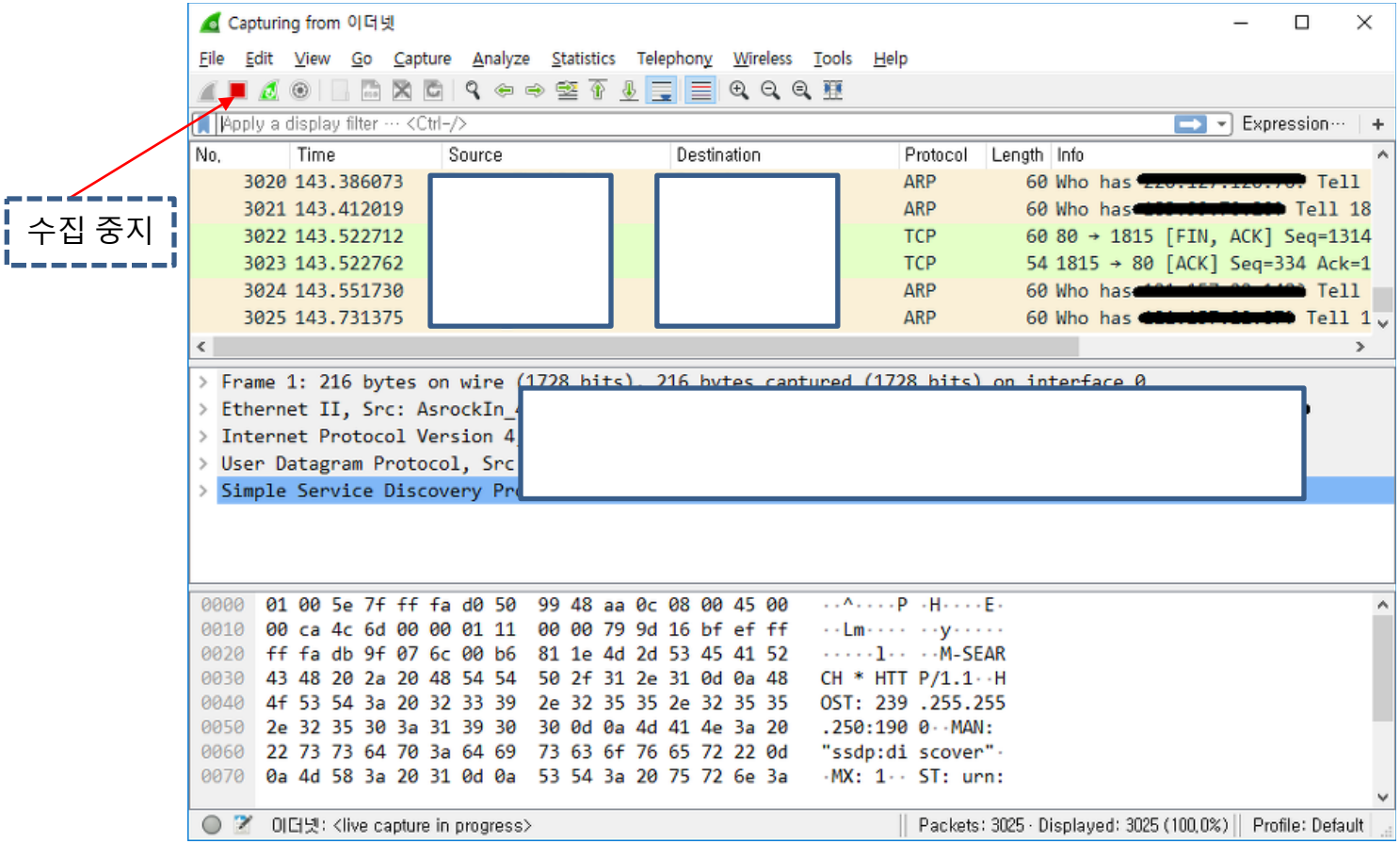


패킷 캡처 시작

이더넷 인터페이스 선택

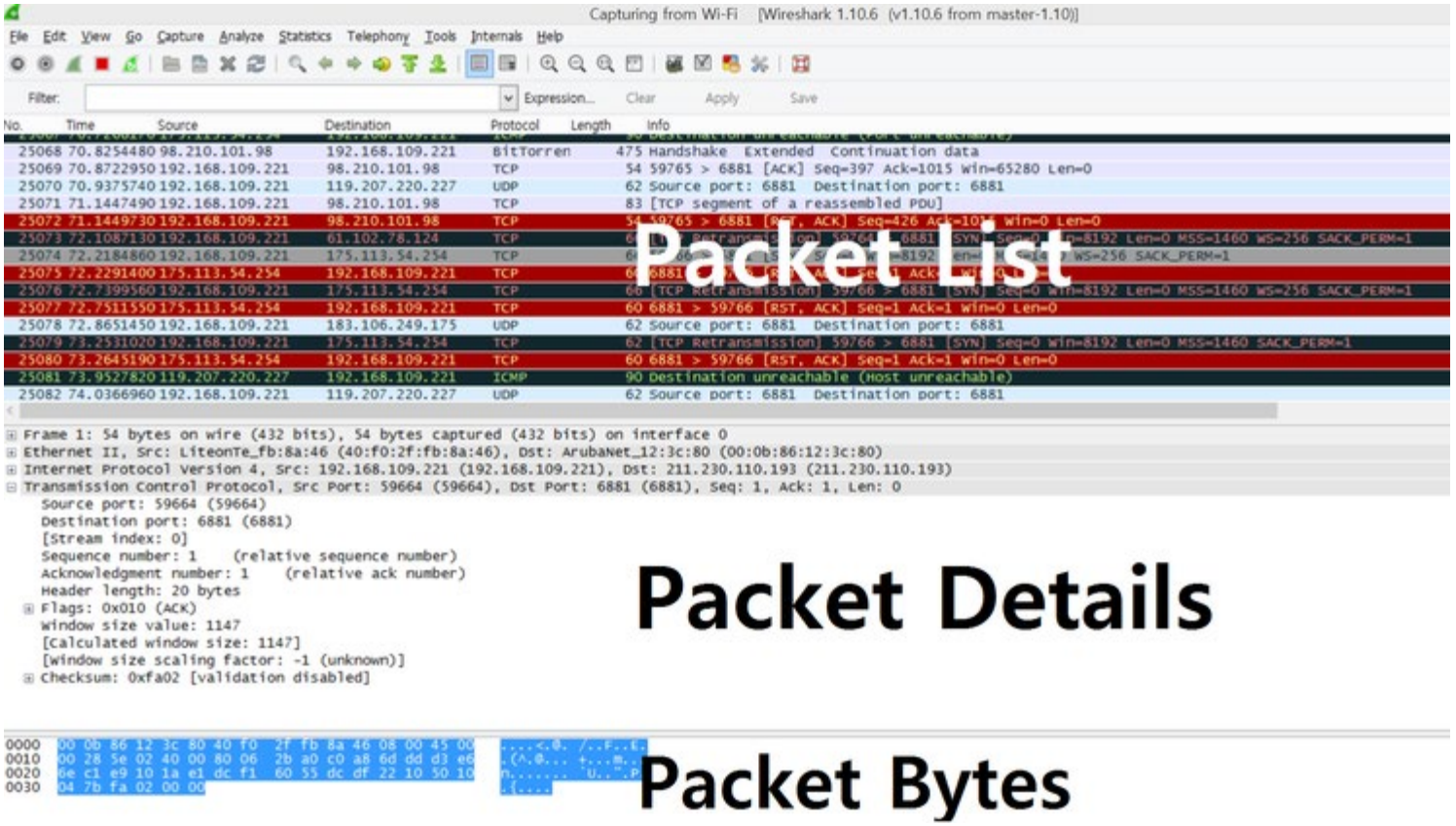
WireShark 실행

- **패킷 캡처**



WireShark 실행

- **패킷 캡처**

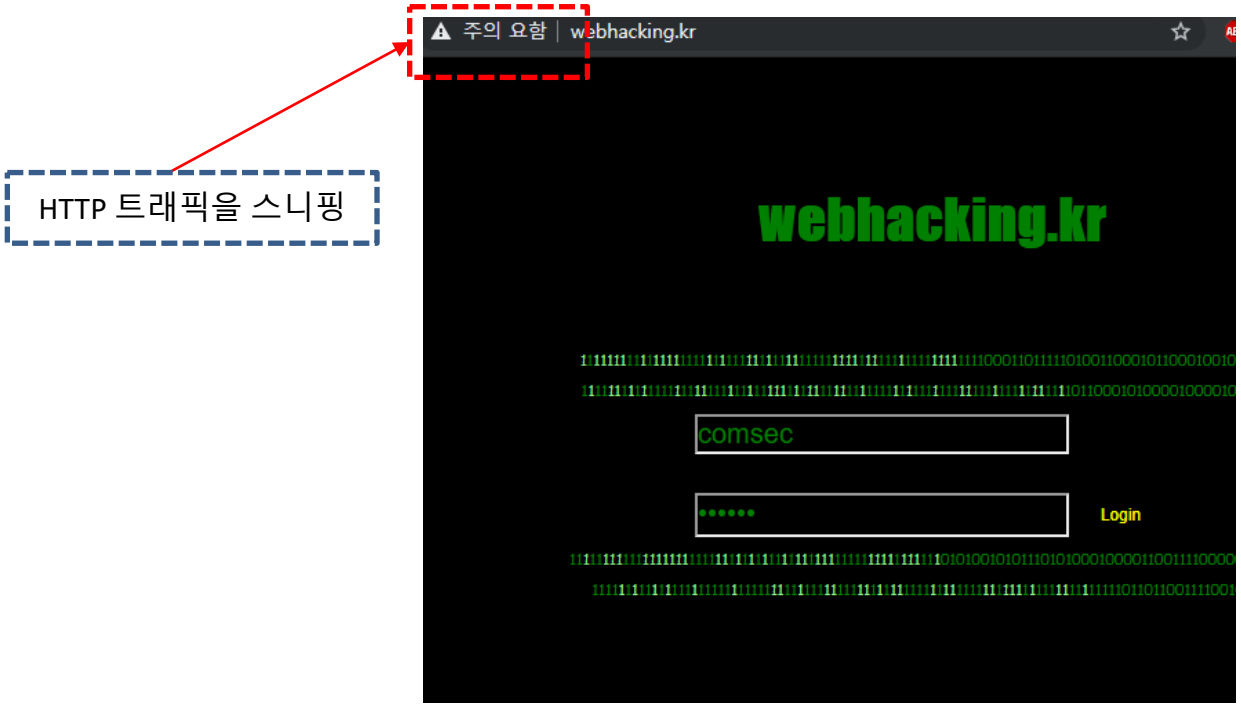


WireShark 실습

1. HTTP 패킷 캡처 분석

→ http://webhacking.kr 접속

→아이디와 비밀번호 입력, 로그인 누르지 않고 와이어샤크 실행

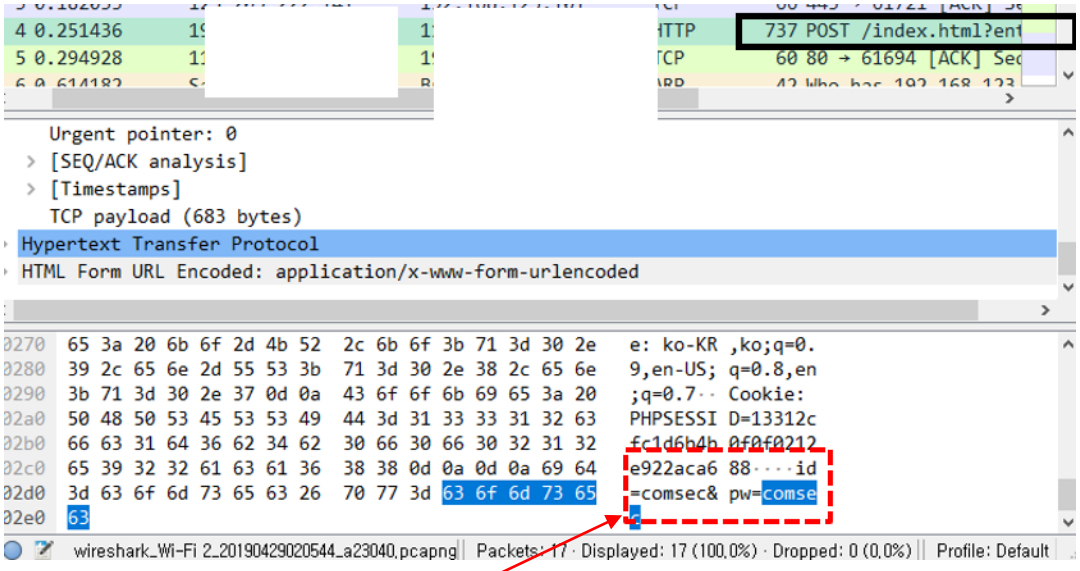


WireShark 실습

1. HTTP 패킷 캡처 분석

→ 로그인 시도, 이후 패킷 수집 중지

→ 패킷들 사이에서 ID/PW 확인



암호화 되지 않은 평문으로 전송 확인

WireShark 실습

1. HTTP 패킷 캡처 분석

→ HTTP 프로토콜 취약점으로 인하여 패킷 스니핑 당할 경우 위험 노출

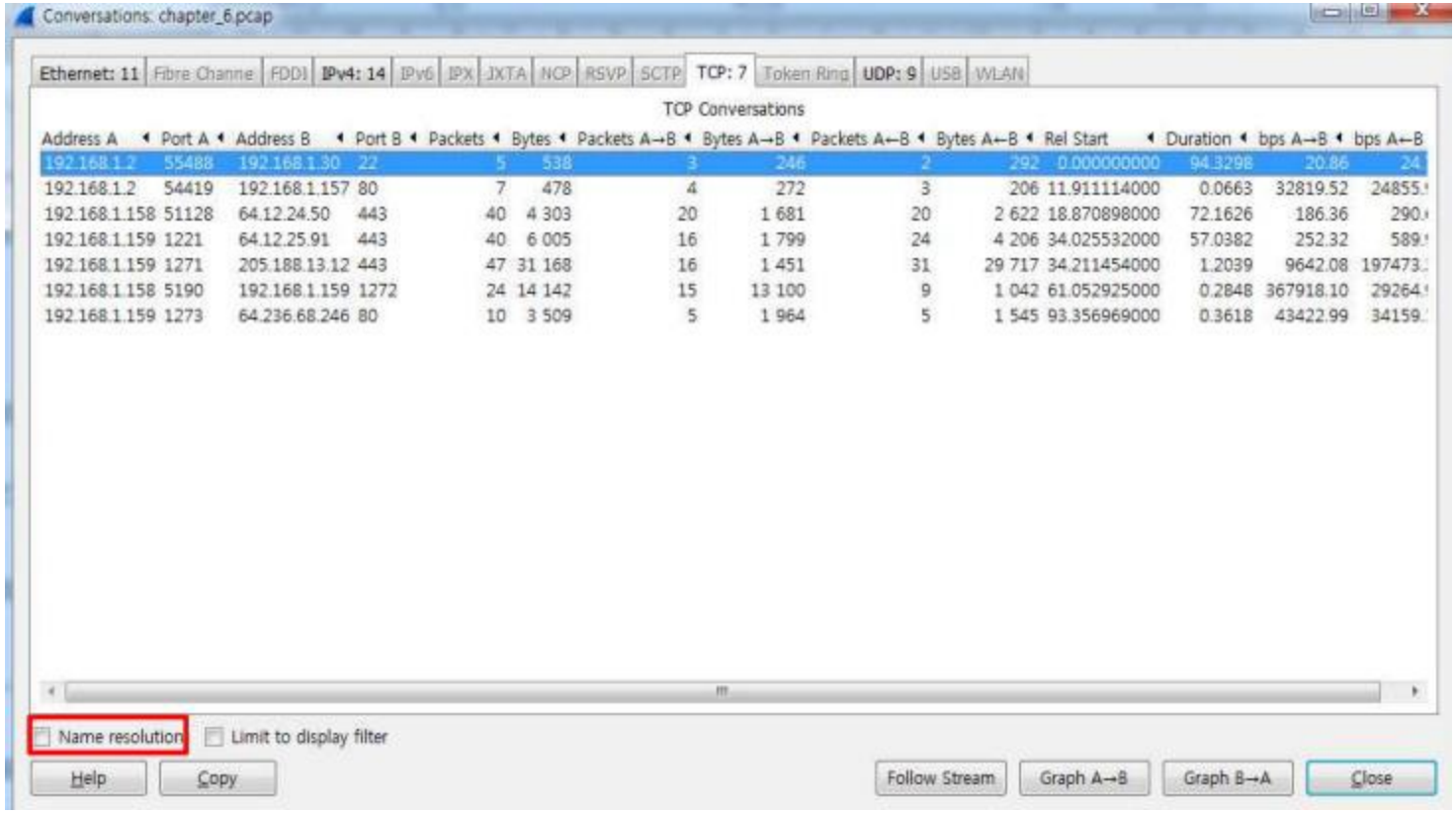
- HTTPS 패킷 분석

→ SSL로 인한 암호화로 정보 획득 어려움

→ 이후 SSL Strip등 여러 공격 툴 개발, 추가적인 RSA암호화

와이어샤크

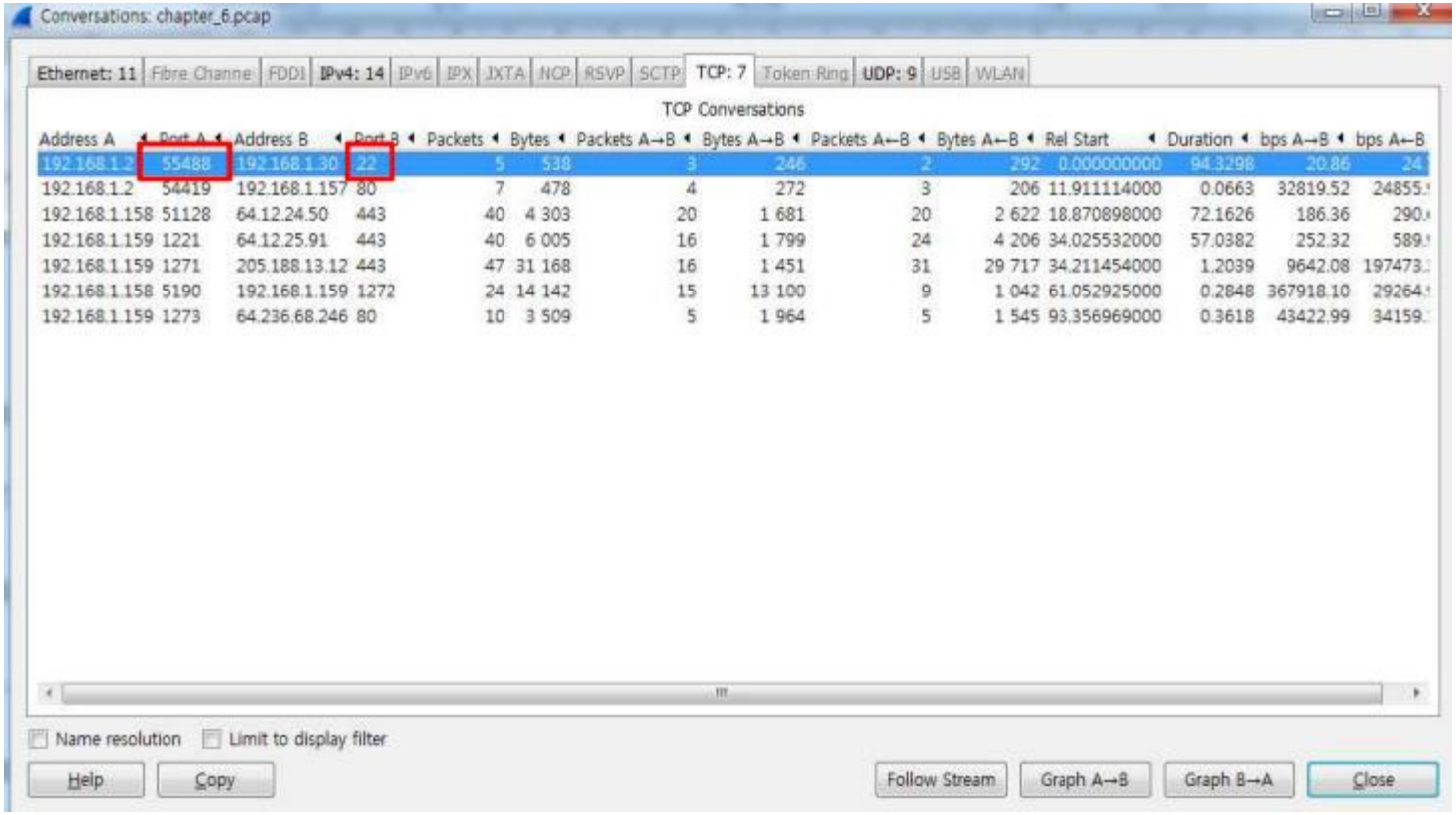
- Conversations



- 메뉴 [statistics] – [Conversations]를 클릭하고, 포트를 이름으로 보는 대신 번호로 확인하기 위해 하 단의 [Name Resolution]을 체크오프 합니다

와이어샤크

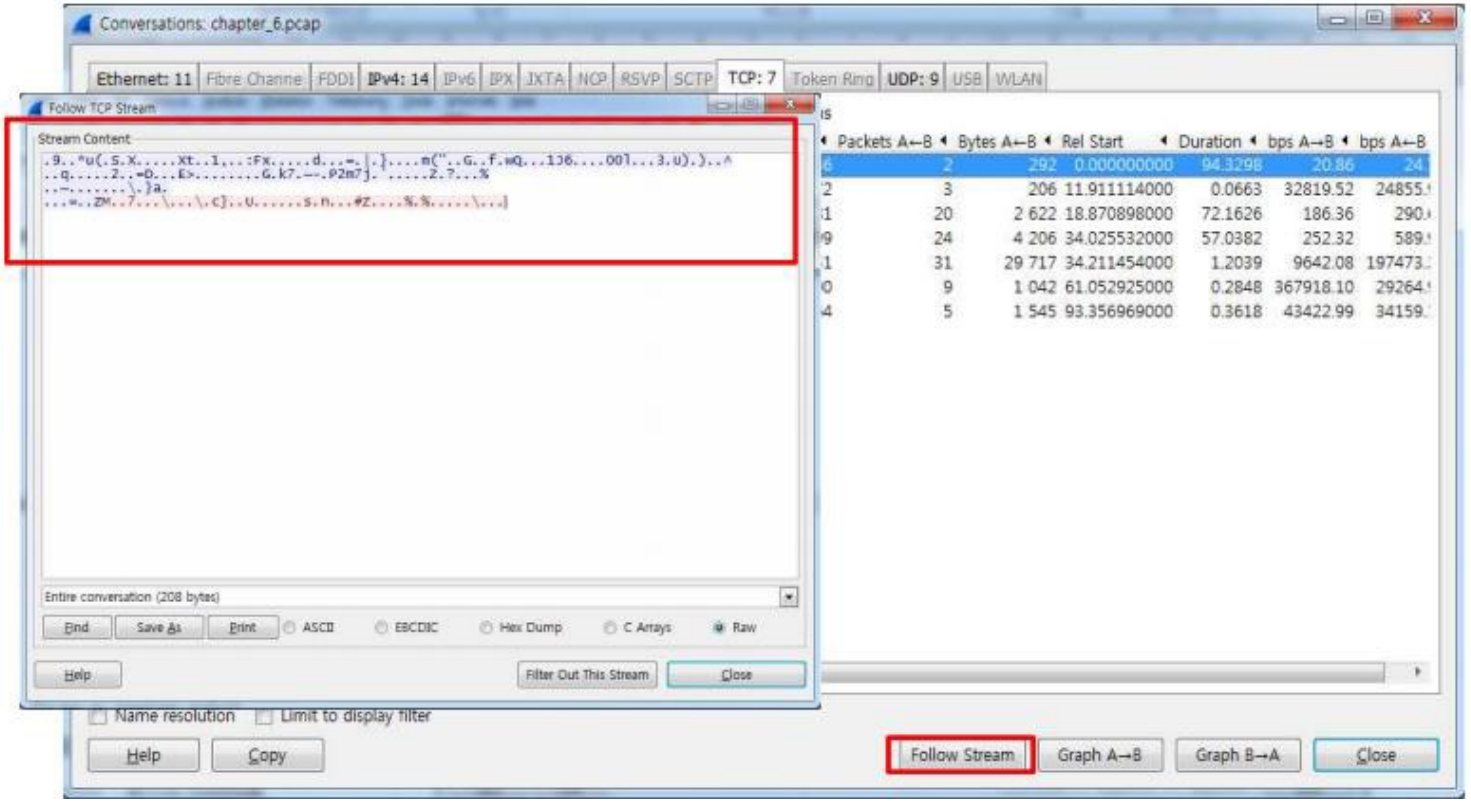
- Conversations



- 첫 번째 세션의 경우, 통신의 방향은 Port A 55488에서 Port 22로 접속한다는 것을 알 수 있는데, TCP 22번은 Telnet 등의 평문데이터를 보호하기 위해 암호화 처리하는 프로토콜이다.

와이어샤크

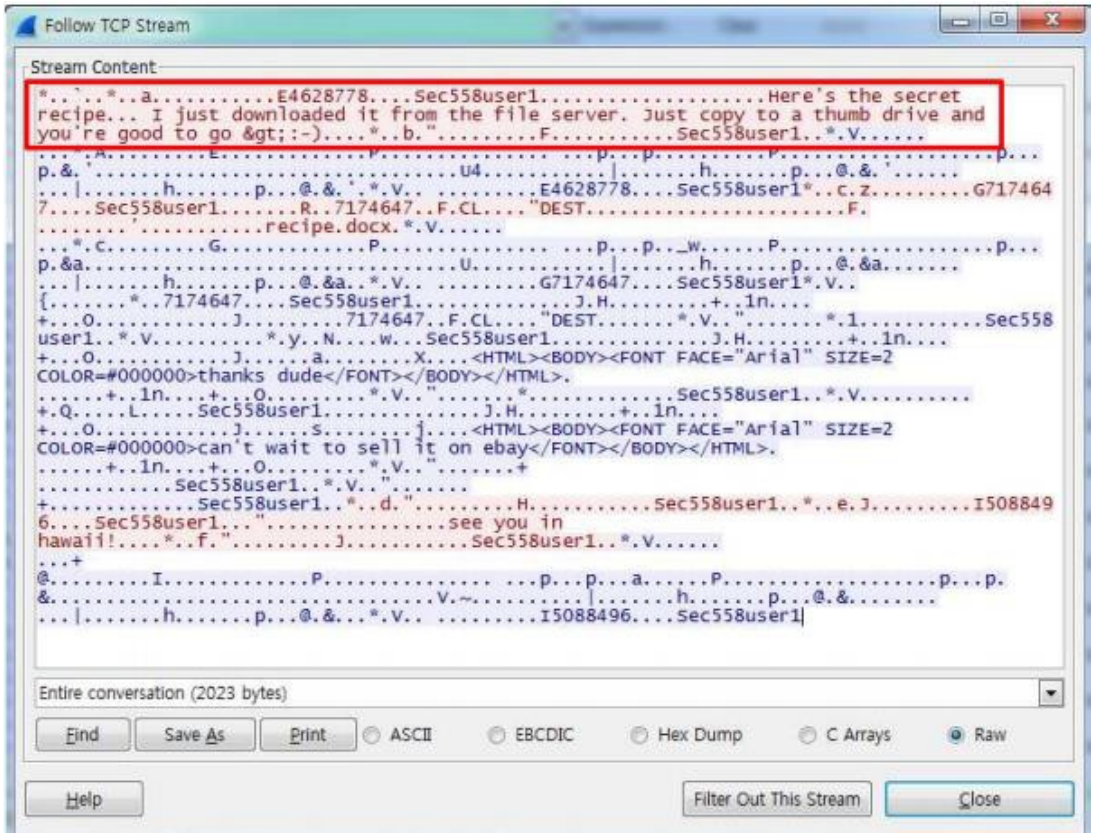
- Follow Stream



- 하단의 [Follow Stream] 클릭을 통해 패킷수집 내용을 확인해보면, 암호화 통신이기 때문에 문자열 확 인이 불가능하다. .

와이어샤크

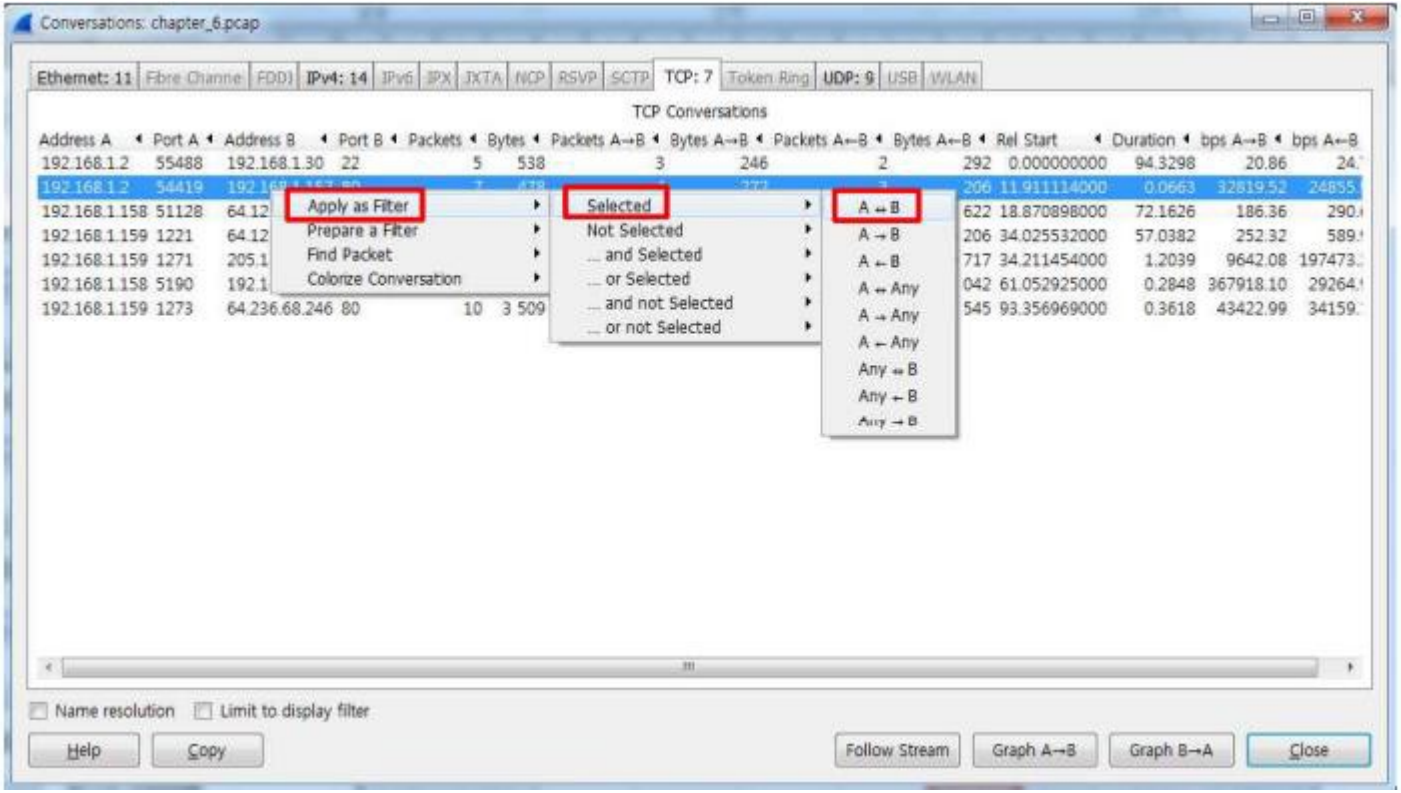
- Follow Stream



- 일부패킷은 [Follow stream]으로 확인해보면 HTTPS 통신임에도 불구하고, 일부 확인할 수 있는 문자열 등이 보인다.

와이어샤크

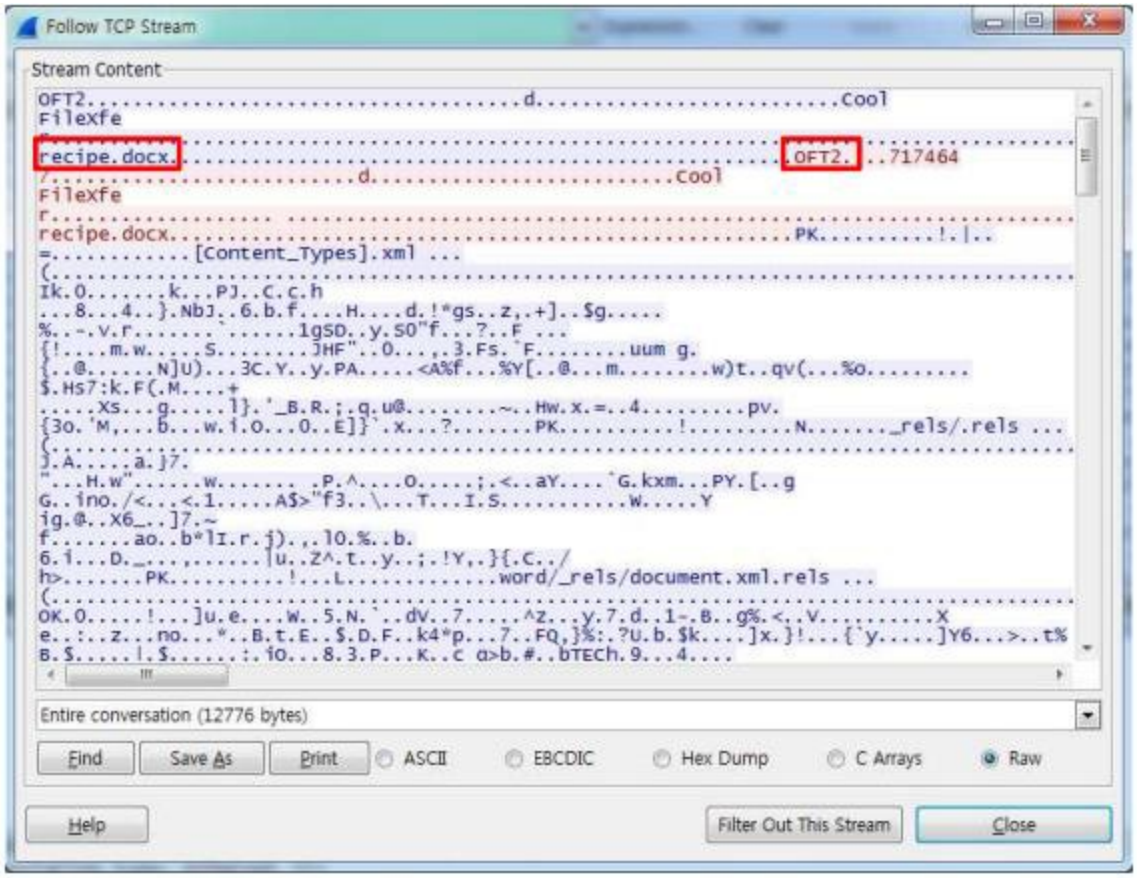
- Follow Stream



- 확인되지 않는 패킷정보는 필터링을 통해 상세분석 할 수있다. 아래 패킷에서 마우스 우클릭, [Apply as Filter]-[Selected]-[A<->B]를 클릭

와이어샤크

- 분석을 통한 파일 추출

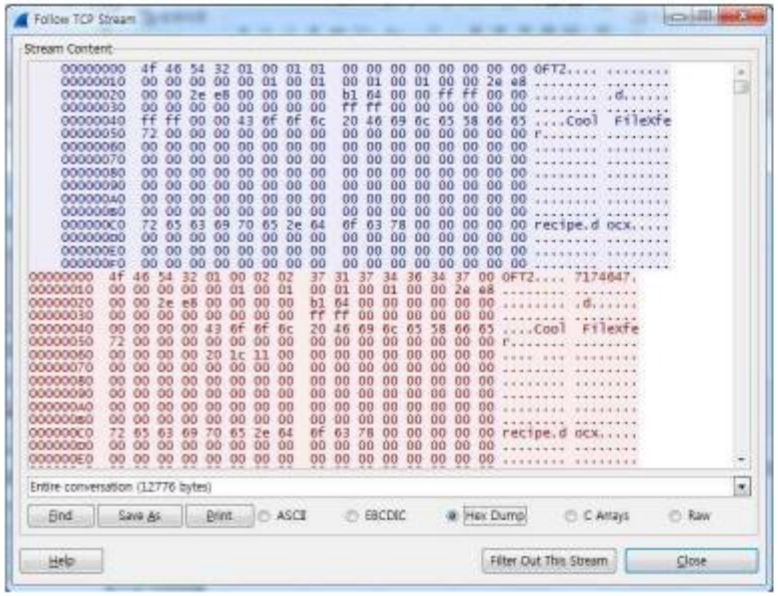


[Follow Stream]을 통해 확인해 보면 OFT2 및 recipe.docx 등의 정보가 보이는 것을 알 수 있다.

와이어샤크

- 분석을 통한 파일 추출

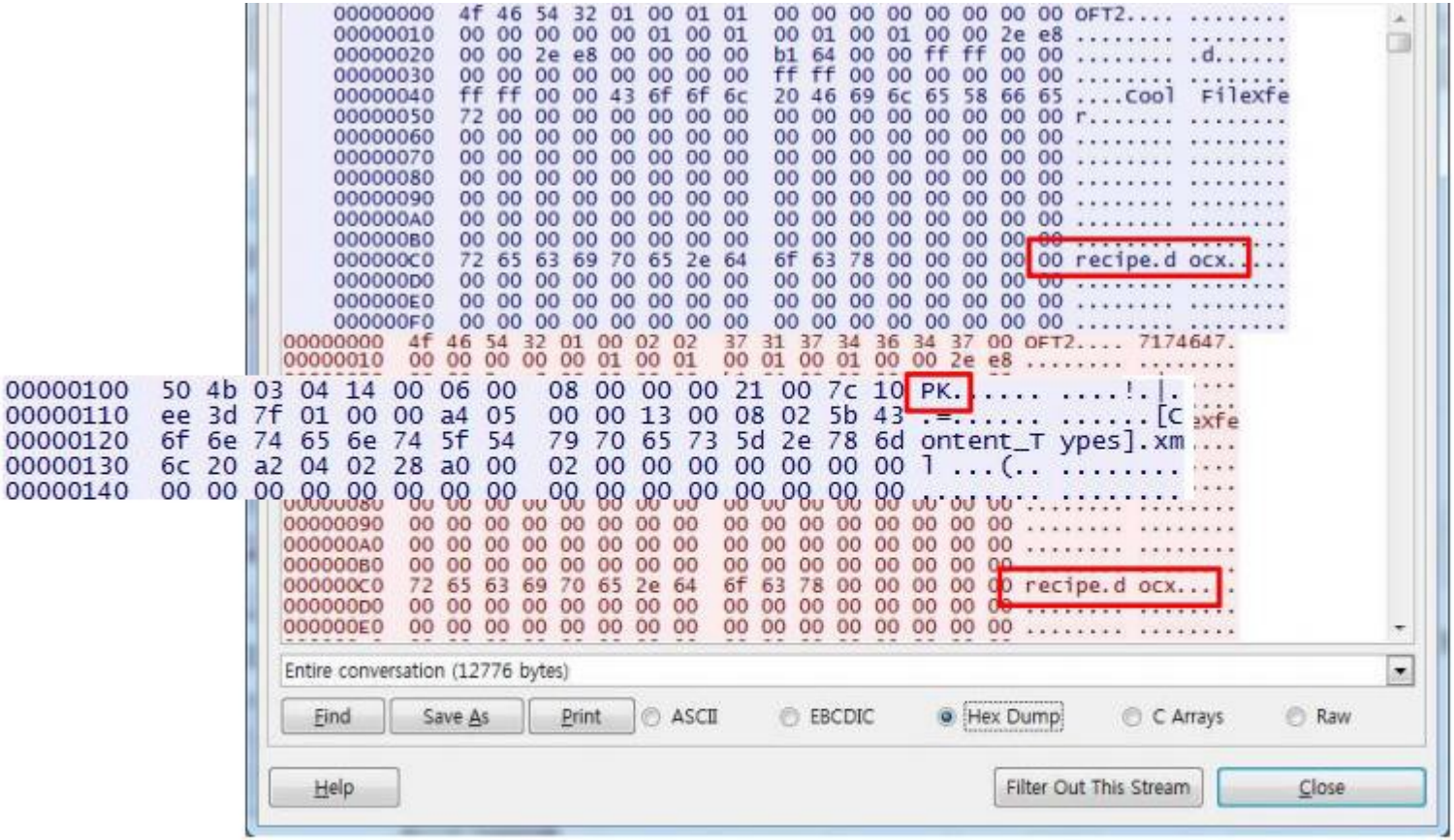
해당 [Follow Stream] 구조를 다른 포맷으로 확인하여, 어던 정보들의 조합인지를 쉽게 확인해 볼 수 있는데, 대표적인 것이 Hex Dump라는 것이다.



Hex Dump를 체크하고 보면 색상이 다르게 구분된 것이 총 4개라는 것을 볼 수 있다.

와이어샤크

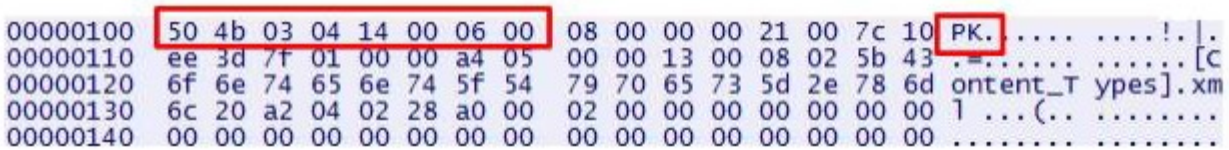
- 분석을 통한 파일 추출



OFT2는 메신저 통신내용으로 4개 중 3개를 차지하고 있는데, OFT2 블록마다 recipe.docx라는 문자열이 보인다. 여기서 세 번째 블록에 보이는 "PK"라는 문자열은 Magic Number 라는 값이다.

와이어샤크

- 분석을 통한 파일 추출



검색페이지에서 PK의 16진수 값 뒤에 함께 오는 값을 검색해 보면,
OFFICE 계열의 포멧이라는 것을 확인할 수가 있다.

50 4B 03 04 14 00 06 00
DOCX, PPTX, XLSX

PK.....
Microsoft Office Open XML Format (OOXML) Document
NOTE: There is no subheader for MS OOXML files as there is with DOC, PPT, and XLS files. To better understand the format of these files, rename any OOXML file to have a .ZIP extension and then unZIP the file; look at the resultant file named *[Content_Types].xml* to see the content types. In particular, look for the *<Override PartName=* tag, where you will find *word*, *ppt*, or *xl*, respectively.

Trailer: Look for 50 4B 05 06 (PK..) followed by 18 additional bytes at the end of the file.

이로써 해당 블록이 OFT2 블록에서 보였던 recipe.docx라고 가정하고 접근해 볼 수 있다.

와이어샤크

- 분석을 통한 파일 추출

```
00000100  50 4b 03 04 14 00 06 00  08 00 00 00 21 00 7c 10  PK.. .... ....!.|.
00000110  ee 3d 7f 01 00 00 a4 05  00 00 13 00 08 02 5b 43  .=.. .... ......[C
00000120  6f 6e 74 65 6e 74 5f 54  79 70 65 73 5d 2e 78 6d  ontent_T ypes].xm
00000130  6c 20 a2 04 02 28 a0 00  02 00 00 00 00 00 00 00  l ...(.. ........
00000140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
```

PCAP 포멧의 구조체에서 언급한 Magic Number라고 언급했었다. 파일포멧마다 고유의 Magic Number를 가지고 있어, 이를 통해 패킷 내에 포함된 파일종류를 확인하고, 추출해낼 수가 있다.

http://www.garykessler.net/library/file_sigs.html

위의 URL에서 파일포멧의 종류를 검색해 볼 수 있다.

와이어샤크

- **Quiz 01 문제**
- 문제 및 파일
- http://twodragon.tistory.com/455

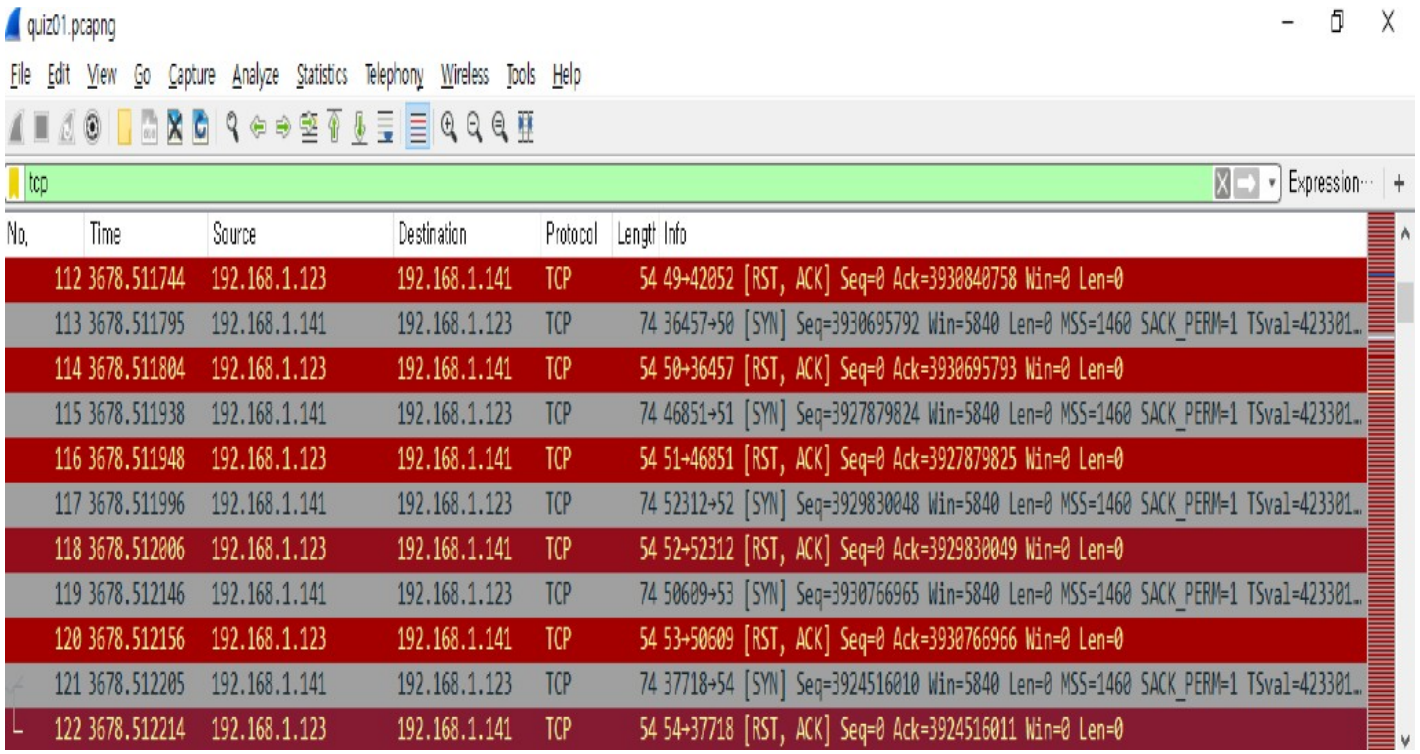
  – 본 캡처 파일은 매우 오랫동안 Packet Dump를 받아 놓은 파일이다.
  – 네트워크 관리자의 생각으로는 의심스러운 무언가가 포함 되어 있다고 생각하고 있어 당신에게 해당 파일 분석 요청했다.

1. 공격자 호스트의 IP 주소는 무엇인가?
2. 대상 호스트의 IP 주소는 무엇인가?
3. 대상의 어떤 TCP 포트가 열려 있는가??
4. 어떤 ICMP의 비 표준형 / 코드 번호가 포함되어 있는가?
5. 대상을 스캔 하는데 어떤 소프트웨어를 사용 하였는가?

와이어샤크

- **Quiz 01 문제풀이**

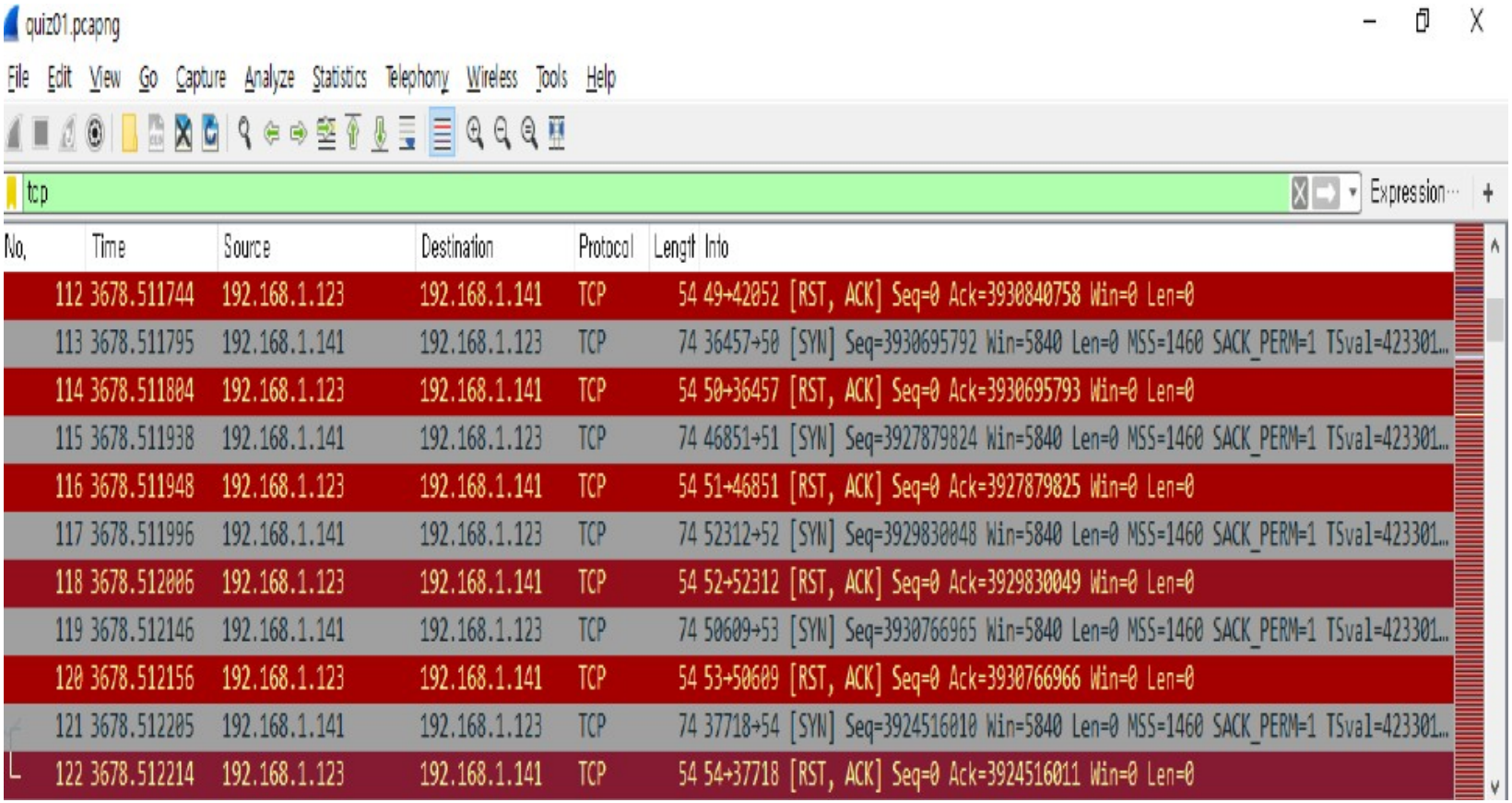
1. 공격자 호스트의 IP 주소는 무엇인가?



와이어샤크

- **Quiz 01 문제풀이**

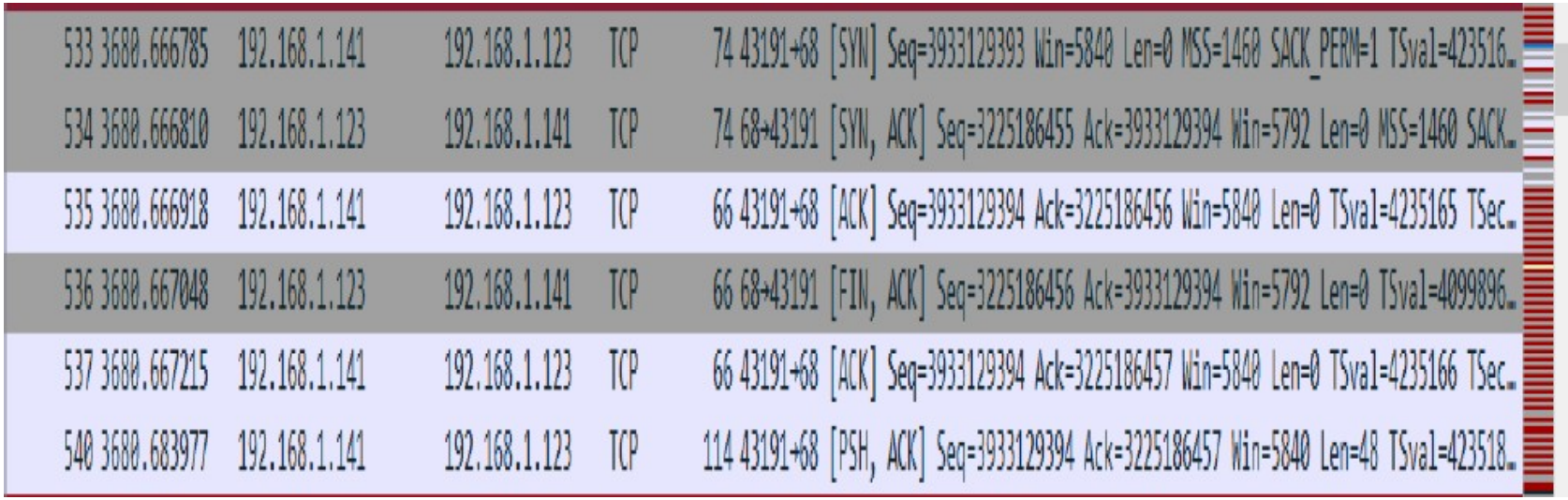
2. 대상 호스트의 **IP** 주소는 무엇인가**?**



와이어샤크

- **Quiz 01 문제풀이**

3. 대상의 어떤 **TCP** 포트가 열려 있는가**??**

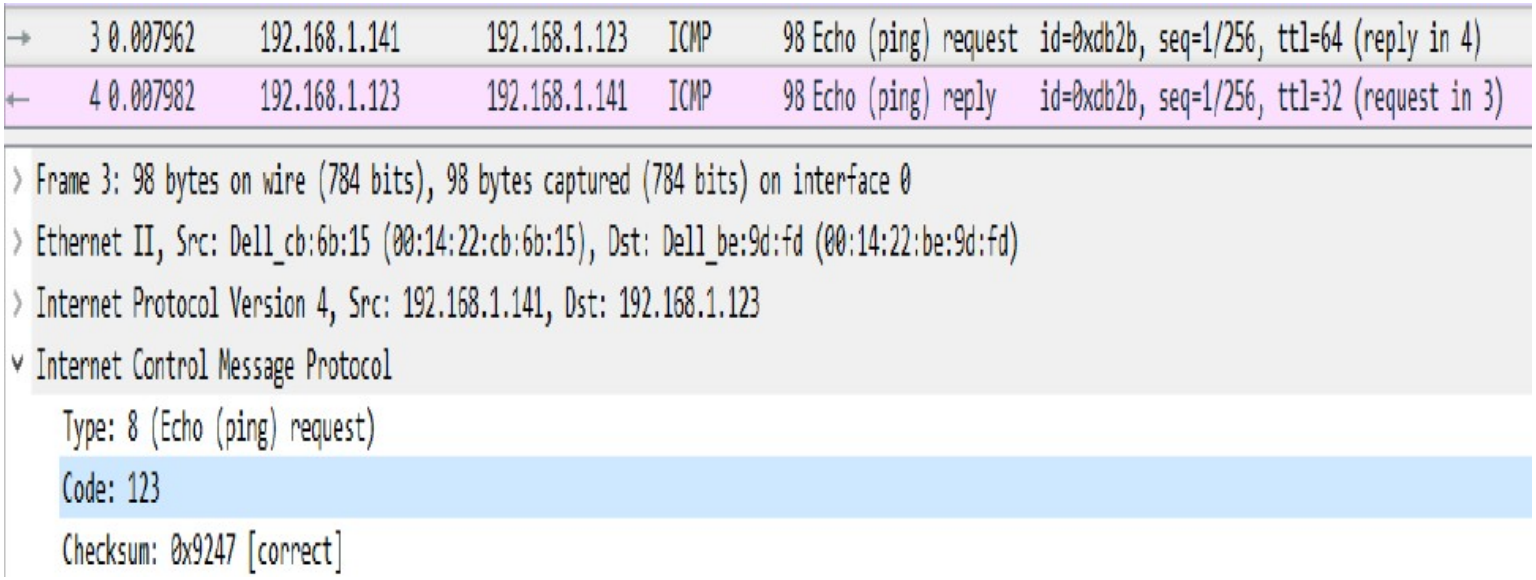


533 3688.666785	192.168.1.141	192.168.1.123	TCP	74 43191→68 [SYN] Seq=3933129393 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=423516…
534 3688.666810	192.168.1.123	192.168.1.141	TCP	74 68→43191 [SYN, ACK] Seq=3225186455 Ack=3933129394 Win=5792 Len=0 MSS=1460 SACK…
535 3688.666918	192.168.1.141	192.168.1.123	TCP	66 43191→68 [ACK] Seq=3933129394 Ack=3225186456 Win=5840 Len=0 TSval=4235165 TSec…
536 3688.667048	192.168.1.123	192.168.1.141	TCP	66 68→43191 [FIN, ACK] Seq=3225186456 Ack=3933129394 Win=5792 Len=0 TSval=4099896…
537 3688.667215	192.168.1.141	192.168.1.123	TCP	66 43191→68 [ACK] Seq=3933129394 Ack=3225186457 Win=5840 Len=0 TSval=4235166 TSec…
540 3688.683977	192.168.1.141	192.168.1.123	TCP	114 43191→68 [PSH, ACK] Seq=3933129394 Ack=3225186457 Win=5840 Len=48 TSval=423518…

와이어샤크

- **Quiz 01 문제풀이**

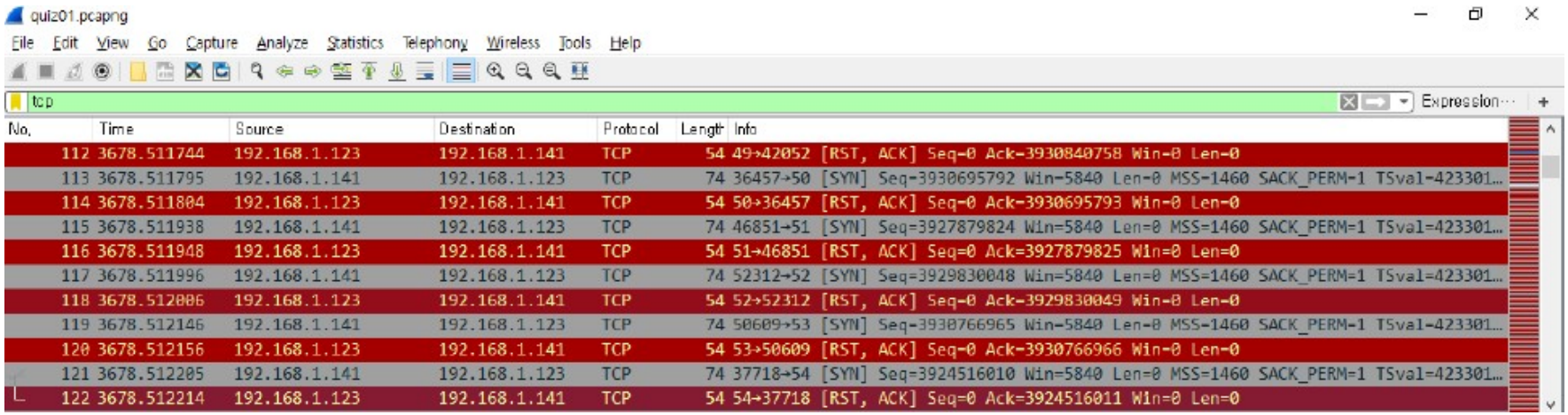
4. 어떤 **ICMP**의 비 표준형 / 코드 번호가 포함되어 있는가**?**



와이어샤크

- **Quiz 01 문제풀이**

5. 대상을 스캔 하는데 어떤 소프트웨어를 사용 하였는가?



와이어샤크

- **Quiz 02 문제**
- 문제 및 파일

- http://twodragon.tistory.com/455

  – 본 캡처 파일은 "제로 데이"공격을 경험 네트워크에서 가져온 Packet Dump 파일이다. 네트워크 관리자는 당신에게 분석 요청했다.관리자는 141.157.228.12이 서버이고, 10.1.1.31있는 클라이언트 시스템이다.

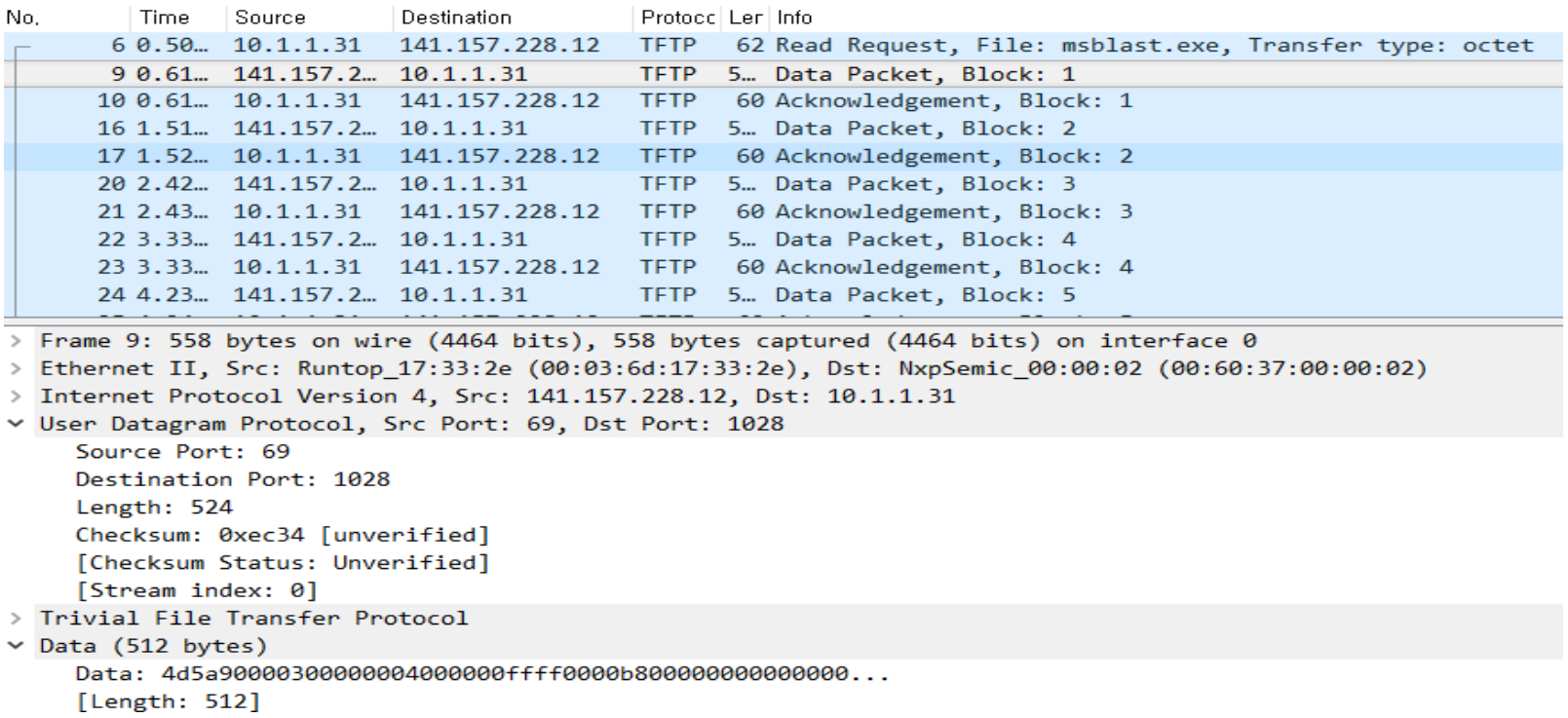
1. 어떤 응용 프로그램을 이용하여 파일을 전송 하였는가?
2. 파일을 수신하는 호스트의 IP 주소는 무엇인가?
3. 전송되는 파일의 이름은무엇입니까?

와이어샤크

- **Quiz 02 문제풀이**

1) 어떤 응용 프로그램을 이용하여 파일을 전송하였는가?

Tftp를 통하여 파일을 전송하는 모습이다.



No.	Time	Source	Destination	Protocc	Ler	Info
6	0.50…	10.1.1.31	141.157.228.12	TFTP	62	Read Request, File: msblast.exe, Transfer type: octet
9	0.61…	141.157.2…	10.1.1.31	TFTP	5…	Data Packet, Block: 1
10	0.61…	10.1.1.31	141.157.228.12	TFTP	60	Acknowledgement, Block: 1
16	1.51…	141.157.2…	10.1.1.31	TFTP	5…	Data Packet, Block: 2
17	1.52…	10.1.1.31	141.157.228.12	TFTP	60	Acknowledgement, Block: 2
20	2.42…	141.157.2…	10.1.1.31	TFTP	5…	Data Packet, Block: 3
21	2.43…	10.1.1.31	141.157.228.12	TFTP	60	Acknowledgement, Block: 3
22	3.33…	141.157.2…	10.1.1.31	TFTP	5…	Data Packet, Block: 4
23	3.33…	10.1.1.31	141.157.228.12	TFTP	60	Acknowledgement, Block: 4
24	4.23…	141.157.2…	10.1.1.31	TFTP	5…	Data Packet, Block: 5

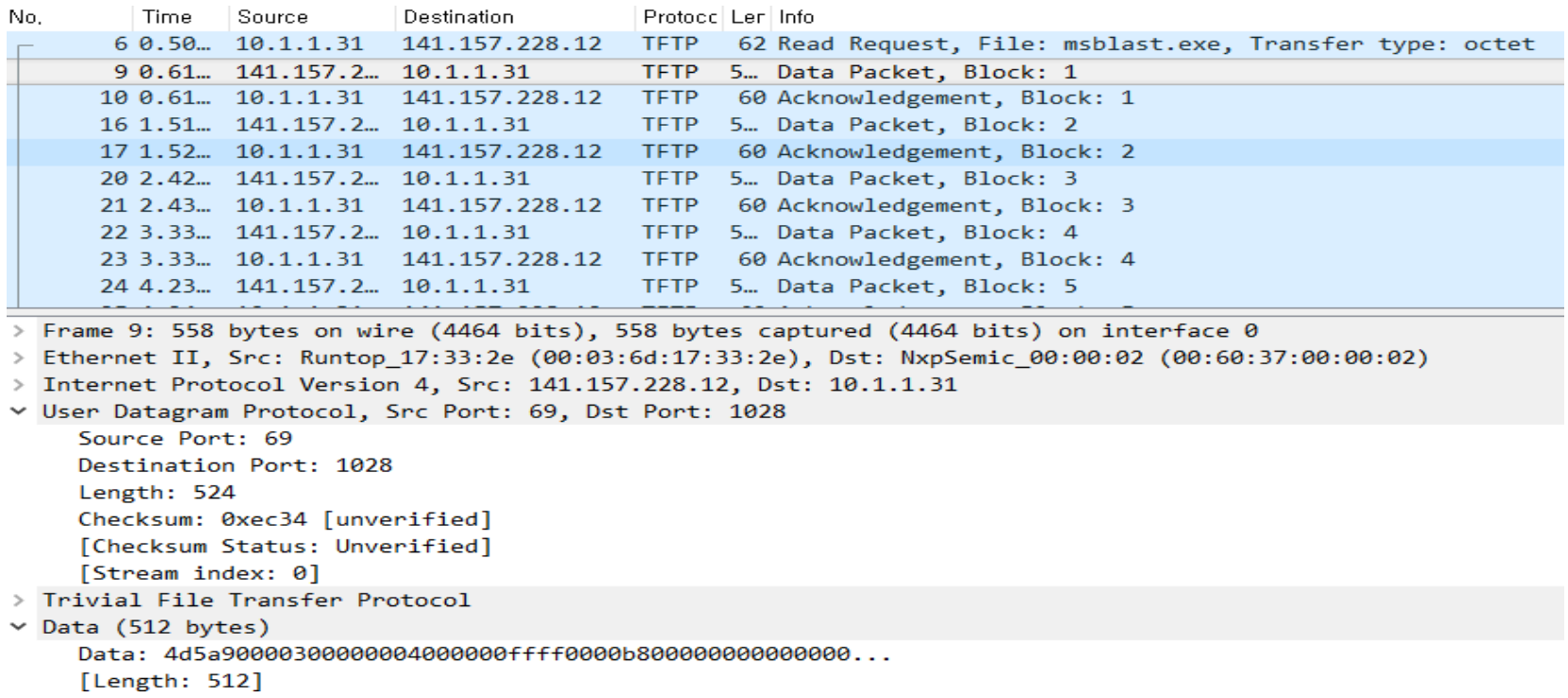
```
> Frame 9: 558 bytes on wire (4464 bits), 558 bytes captured (4464 bits) on interface 0
> Ethernet II, Src: Runtop_17:33:2e (00:03:6d:17:33:2e), Dst: NxpSemic_00:00:02 (00:60:37:00:00:02)
> Internet Protocol Version 4, Src: 141.157.228.12, Dst: 10.1.1.31
v User Datagram Protocol, Src Port: 69, Dst Port: 1028
    Source Port: 69
    Destination Port: 1028
    Length: 524
    Checksum: 0xec34 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
> Trivial File Transfer Protocol
v Data (512 bytes)
    Data: 4d5a900003000000040000000ffff0000b800000000000000...
    [Length: 512]
```

와이어샤크

- **Quiz 02 문제풀이**

2) 파일을 수신하는 호스트의 IP 주소는 무엇인가?

141.157.228.12 -> 10.1.1.31 에서 파일을 수신을 받고 있음

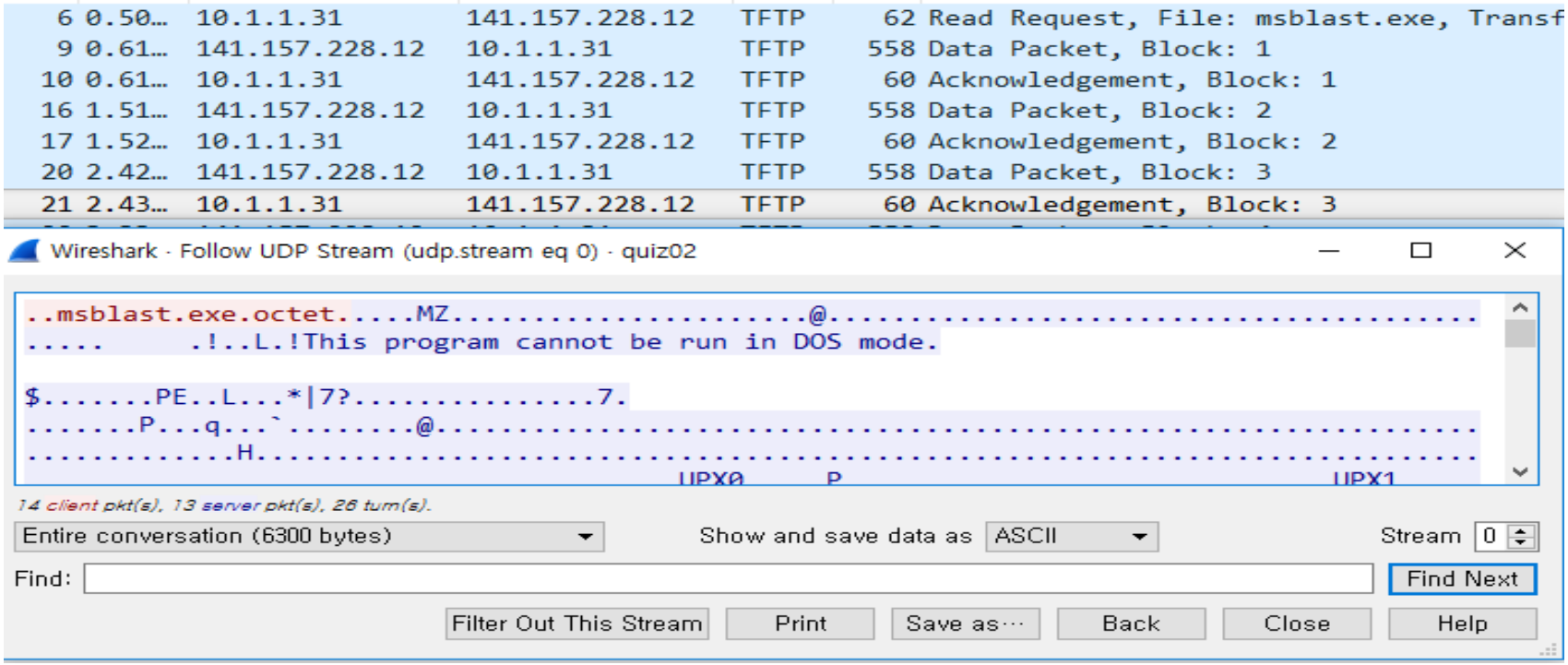


와이어샤크

- **Quiz 02 문제풀이**

3) 전송되는 파일의 이름은 무엇입니까?

- Tftp를 오른쪽 클릭 후에 follow stream UDP로 하였더니 위와 같이 파일의 이름인 msblast.exe 프로그램을 전송



참고문헌

- 정보 보안 개론[개정3판], 양대일 저, 한빛미디어, 2018, 1.
- 디지털 포렌식 개론(2판), 이상진 저, 이룬 출판사, 2015. 5.
- 컴퓨터보안, William Stalling 저, 한티미디어, 2016. 8
- 정보보안과 사이버 해킹의 기초, 김경신 저, 2016. 8

Q & A