Computer Network Assignment #1

2018380603 정이든

두 end host인 VM1, VM3의 interface Setup을 마친 후, 각각의 머신에서 서버, 클라이언트 소켓 프로그램을 작성 하였습니다. 그리고 컴파일을 한 후 프로그램을 실행함으로써 패킷을 보냈습니다.

다음은 VM1의 터미널에서 TCP client program을 작성한 후, 실행한 결과입니다.
프로그램은 Server/Client가 대화를 주고받다가 "exit" 메시지를 보내면 소켓이 닫히는 형식으로 작성 하였습니다.

```
cnstu@cnstu-VirtualBox:~$ gcc client.c -o client
cnstu@cnstu-VirtualBox:~$ ./client
Socket successfully created..
connected to the server..
Enter the string : Hi 2donny
From Server : hello FAKE don
Enter the string : exit
From Server : exit
Client Exit...
cnstu@cnstu-VirtualBox:~$
```

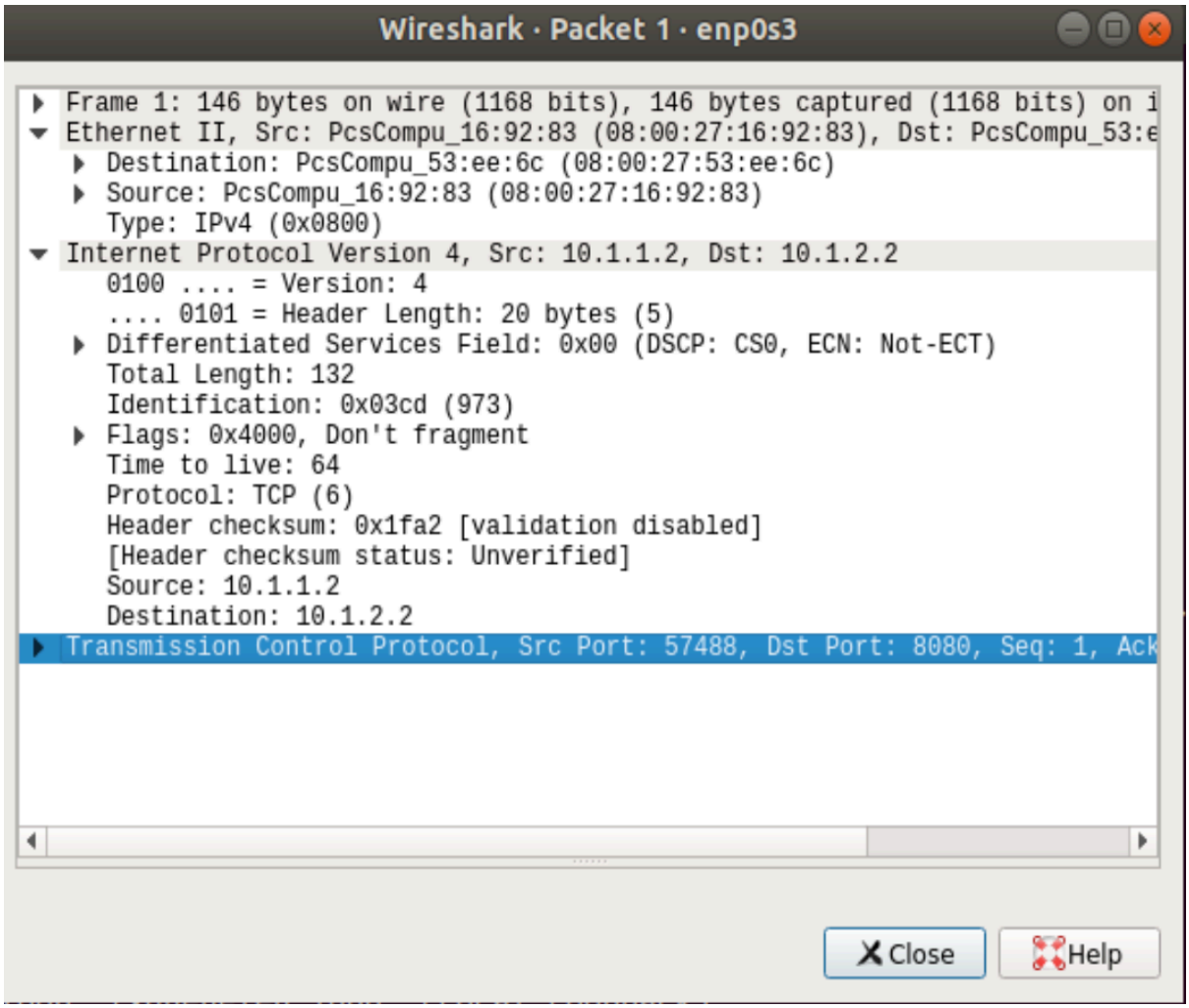
밑의 사진은 VM3에서 TCP Server program을 실행해준 것인데, 이 서버 프로그램을 먼저 실행해주었습니다. 그랬더니 "Server Listening.." 상태에서 멈춰있다가, VM1에서 패킷을 보내니 그제서야 client를 accept하였고 두 소켓이 연결되었습니다.

```
cnstu@cnstu-VirtualBox:~$ ./server
Socket successfully created..
Socket successfully binded..
Server listening..
server acccept the client...
From client: Hi 2donny
        To client : hello FAKE don
From client: exit
        To client : exit
Server Exit...
cnstu@cnstu-VirtualBox:~$
```

1) 패킷 분석

이제 패킷을 분석해 보겠습니다.

VM1에서 캡쳐한 패킷을 분석해 보겠습니다.



이 패킷은 Data Link 계층의 MAC부터 Network 계층의 IP, Trasport 계층의 TCP, Application 계층의 Data까지 담겨있습니다. 그럼 분석해보겠습니다.

EtherType:

Type(IP)는 프레임의 종류 중 IEE 802.3과 Ethernet 2.0으로 구분되는 중요한 필드입니다. Type이 IP이므로 Ethernet 2.0임을 알 수 있습니다. Ethernet에서 IP 헤더와는 다르게 목적지 주소가 먼저 와있는 이유는 브로드 캐스트로 목적지들이 모두 받았을 때 자신 것이 아니면 모두 버리기 때문입니다. 즉, 출발지 주소가 앞에 왔었다면 출발지 주소를 읽고 목적지 주소를 읽어야하는 과정이기 때문에 이는 시간상 리스크가 큽니다.

Ethernet, IP protocol

먼저 MAC과 IP protocol를 Src와 Dst로 나누어 살펴보겠습니다. 먼저 Mac protocol의 "Src Mac"같은 경우에는 송신한 인터페이스의 할당된 식별 주소입니다. VM1에서 송신한 'enp0s3' 인터페이스의 맥주소인 08:00:27:16:92:83와 동일한 것을 확인할 수 있습니다. 그리고 IP protocol의 Src address는 송신한 인터페이스의 IP 주소이므로 10.1.1.2임을 확인할 수 있습니다.

동일한 맥락으로 Dst Mac은 수신하는 인터페이스의 네트워크 주소입니다. 이 패킷에서 수신자의

맥주소는 VM2의 인터페이스이고, 이것의 주소는 08:00:27:53:ee:6c 이므로 일치합니다.
IP protocol의 Dst address같은 경우는 수신자의 IP 주소이기 때문에 VM3의 Ip 주소인 10.1.2.2로 위의 사진과 동일합니다.

IP Protocol 내의 각 필드를 분석해보겠습니다.

- IP version : 처음의 16진수 문자는 IP의 버전을 나타냅니다. 버전은 4, 6이 있습니다. 송신지의 IP 버전과 수신지의 IP버전이 다를 때 수신지에서 지원이 안될 경우 통신이 불가능하게 됩니다. 위에서는 버전 4이기때문에. 0100로 표기되어있습니다.

- IP Header Length : 두번째 16진수 문자(4비트)입니다. 값의 단위는 4바이트로서 필드 값이 1이라면 4바이트를 의미합니다. IP 헤더는 옵션이 없는 경우 일반적으로 5입니다(5 * 4 = 20 바이트).

- Type of service(0) : Differentiated Services codepoint, Explicit Congestion Notification 모든 값들이 0으로 설정되어 있는 상태입니다. 처음의 3비트는 우선수위 8단계를 결정하고, 다음 4비트는 Delay, 처리율, 신뢰성, 비용 중 어떠한 것을 우선시 할 지에 대한 것들을 정하게 됩니다.

- Total Length(132) : IP Porotocol header에 데이터를 포함한 IP Packet의 전체 길이, 전체 데이터그램의 길이를 의미합니다. 단위는 바이트입니다.

- Identification(0x931c(37660)) : 이는 호스트가 연속적으로 전송되는 Datagram을 식별하기 위한 번호입니다. Identification 필드값이 같은 패킷은 원래 같은 데이터 였지만 분할되어 전송되었음을 의미하게 됩니다. 이는 호스트측에 다시 모여 결합되는데 사용합니다.

- Flags(0x4000) : 단편화된 조각들 중 하나라도 손실되어 수신되지 않을 경우 에러가 되어 모두 폐기합니다. FLAG 부분은 처음 3비트로 구성되어 있습니다. 첫째 비트 0고정, 두번째 비트는 Don't 세번째 비트는 More입니다. Don't의 경우 1로 설정되어 있다면 더이상 단편화가 진행되어 있지 않음을 알려줍니다. More의 경우 1로 설정되어 있다면 이번 조각 이후에도 단편화 조각이 더 있다는 것을 알려줍니다. 위 패킷의 경우에는 Don't입니다.

- Time To Live(64) : 데이터그램이 살아 있는 시간을 조절해주는 장치입니다 IP 데이터그램은 일정 수의 토큰을 채워넣고 라우터를 지날 때마다 토큰 수가 감소합니다.

- 프로토콜(TCP) : 어떤 상위 프로토콜이 현재 IP 데이터 그램의 페이로드를 이용하는지 표시합니다. TCP를 알리는 06이 제일 많이 나타납니다. 위에서는 6이므로 TCP 입니다.

- Header checksum(0x1fa2) : IP 헤더의 에러를 점검하는 부분으로 데이터부분은 상위 프로토콜이 처리합니다.

- Src, Dest 주소는 앞에서 다루었으니 생략하겠습니다.

TCP Protocol

TCP 프로토콜의 **Src Port**는 57488인데 이것은, 패킷 송신자인 VM1의 포트번호를 나타냅니다. 그리고 **Dst Port**는 TCP server client program에서 전역변수로 지정한 것과 같아야 하므로 포트번호는 8080입니다.

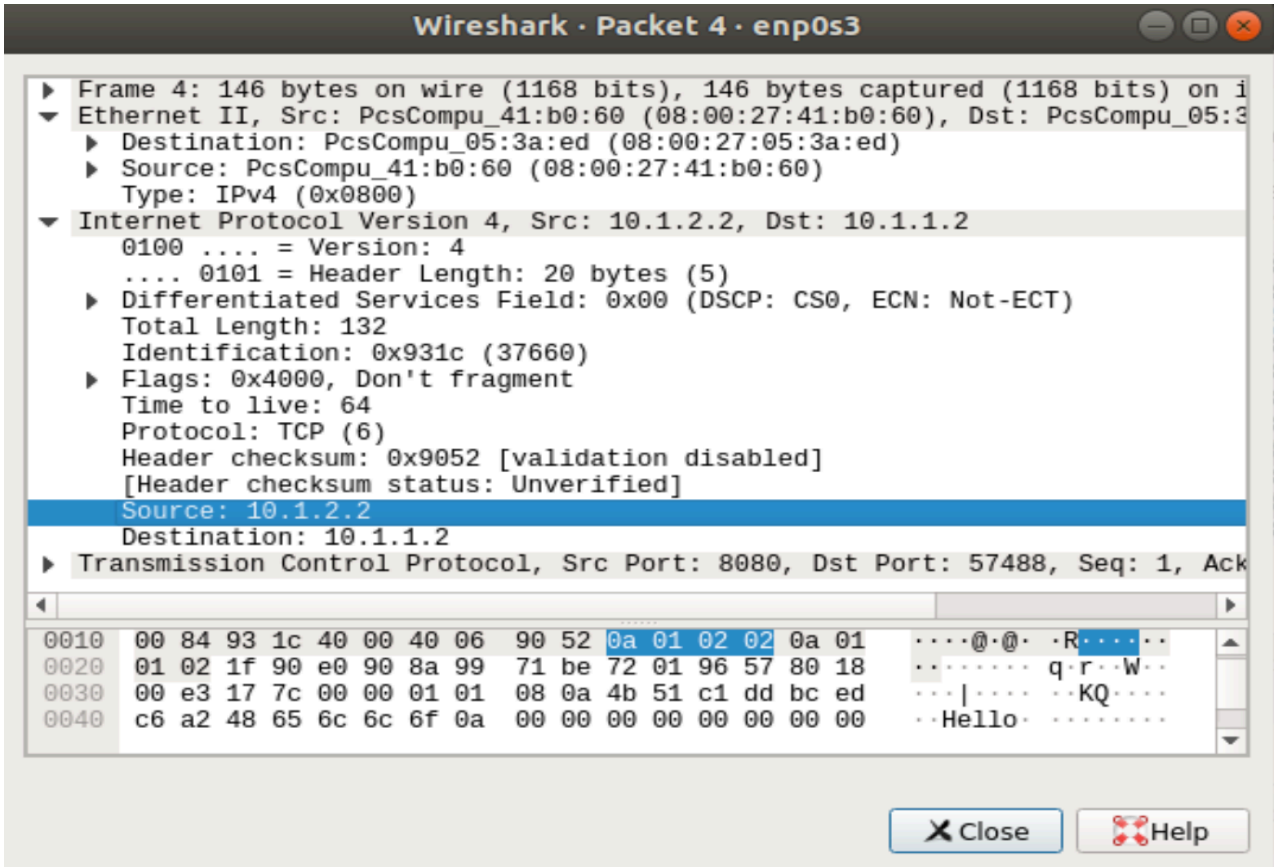
Sequence Number(송신 일련번호) 에서는 신뢰성을 보장하기 위해 세션별로 일련번호를 사용합니다. 3Way-Handshaking에서 사용하는 Sequence 번호인 것이며, 보안적 측면을 위해 랜덤적으로 생성 됩니다. 전송하는 데이터의 각 바이트들을 순서대로 관리합니다.

수신확인 일련번호(Acknowledgement Number) : 3-Way Handshaking 단계 중 상대방으로부터 받기를 기대하는 일련번호입니다. TCP 시작과정에서 첫 번째 단계에서는 서버의 일련 번호를 모르므로 0으로 채웁니다. 따라서 TCP 세션과정에서 찾아내기 위한 용도로 사용됩니다.

TCP 헤더길이 : 처음 4비트는 헤더 길이 필드로서 TCP 헤더 크기를 4바이트 단위로 알립니다. 나머지 필드는 사용하지 않는 보류 필드로서 0으로 채워집니다.

세션 비트 플래그(Flags) : 2비트의 보류 비트 뒤에 6개의 비트를 각각의 플래그로 존재하며 각각 독립적 기능을 합니다.

송신자 윈도우 크기는 수신자로부터 응답을 기다리지 않고 연속적으로 보낼 수 있는 바이트 수입니다.



이 사진은 VM3에서 캡쳐한 패킷입니다. 이것도 분석해보겠습니다.

Ethernet :

- Type(IP)는 프레임의 종류 중 IEE 802.3과 Ethernet 2.0으로 구분되는 중요한 필드입니다. Type이 IP이므로 Ethernet 2.0임을 알 수 있습니다.
- 이 protocol에서의 Src Mac은 송신 인터페이스의 주소이므로 08:00:27:41:b0:60이고 Dest Mac은 수신하는 VM2의 인터페이스의 주소이므로 08:00:27:05:3a:ed 입니다.

IP Protocol 내의 각 필드를 분석해보겠습니다.

- IP version : 처음의 16진수 문자는 IP의 버전을 나타냅니다. 버전은 4와 6이 있습니다. 송신지의 IP 버전과 수신지의 IP버전이 다를 때 수신지에서 지원이 안될 경우 통신이 불가능하게 됩니다. 위에서는 버전 4이기때문에. 0100로 표기되어있습니다.

- IP Header Length(20) : 두번째 16진수 문자(4비트)입니다. 값의 단위는 4바이트로서 필드 값이 1이라면 4바이트를 의미합니다. IP 헤더는 옵션이 없는 경우 일반적으로 5입니다(5 * 4 = 20바이트).

- Type of service(0) : Differentiated Services codepoint, Explicit Congestion Notification 모든 값들이 0으로 설정되어 있는 상태입니다. 처음의 3비트는 우선수위 8단계를 결정하고, 다음 4비트는 Delay, 처리율, 신뢰성, 비용 중 어떠한 것을 우선시 할 지에 대한 것들을 정하게 됩니다.

- Total Length(132) : IP Porotocol header에 데이터를 포함한 IP Packet의 전체 길이, 전체 데이터그램의 길이를 의미합니다. 단위는 바이트입니다.

- Identification(0x931c(37660)) : 이는 호스트가 연속적으로 전송되는 Datagram을 식별하기 위한 번호입니다. Identification 필드값이 같은 패킷은 원래 같은 데이터 였지만 분할되어 전송되었음을 의미하게 됩니다. 이는 호스트측에 다시 모여 결합되는데 사용합니다.

- Flags(0x4000) : 단편화된 조각들 중 하나라도 손실되어 수신되지 않을 경우 에러가 되어 모두 폐기합니다. FLAG 부분은 처음 3비트로 구성되어 있습니다. 첫째 비트 0고정, 두번째 비트는 Don't 세번째 비트는 More입니다. Don't의 경우 1로 설정되어 있다면 더이상 단편화가 진행되어 있지 않음을 알려줍니다. More의 경우 1로 설정되어 있다면 이번 조각 이후에도 단편화 조각이 더 있다는 것을 알려줍니다. 위 패킷의 경우에는 Don't입니다.

- Time To Live(64) : 데이터그램이 살아 있는 시간을 조절해주는 장치입니다 IP 데이터그램은 일정 수의 토큰을 채워넣고 라우터를 지날 때마다 토큰 수가 감소합니다.

- 프로토콜(TCP) : 어떤 상위 프로토콜이 현재 IP 데이터 그램의 페이로드를 이용하는지 표시합니다. TCP를 알리는 06이 제일 많이 나타납니다. 위에서는 6이므로 TCP 입니다.

- Header checksum(0x9052) : IP 헤더의 에러를 점검하는 부분으로 데이터부분은 상위 프로토콜이 처리합니다.

- Src, Dest 주소 : IP protocol의 Src address는 송신한 인터페이스의 IP 주소이므로 10.1.2.2임을 확인할 수 있습니다. IP protocol의 Dst address같은 경우는 수신자의 IP 주소이기 때문에 VM1의 Ip 주소인 10.1.1.2로 위의 사진과 동일합니다.

TCP protocol

TCP 프로토콜의 **Src Port**는 8080인데 이것은, 패킷 송신자 의 포트번호를 나타냅니다. 그리고 **Dst Port**는 수신자 즉, 목적지 주소의 포트번호인 8080입니다.

2) EUI-48 address의 구조

EUI-48은 16진수 6자리로 구성됩니다.
하나의 맥주소 중 상위 24Bit는 제조회사에 할당된 주소이고 하위 24bit(3byte)는 제조 번호에 해당합니다. Mac protocol은 앞서 언급했다시피 6byte의 Dest, Src Mac과 2byte의 Type으로 이루어져있습니다.
VM1에서 캡쳐한 패킷을 먼저 분석하겠습니다.
Src Mac, Dest Mac, Type에 해당하는 16진수 값이 각각
08:00:27:16:92:83, 08:00:27:53:ee:6c, 0x0800으로
EUI-48의 구조가 형성됩니다.

비슷한 맥락으로
VM3에서 캡쳐한 패킷의 EUI-48 address의 구조도
08:00:27:41:b0:60, 08:00:27:05:3a:ed, 0x0800
으로 구조가 형성되어있습니다.

3) TCP connection identifier

연결 식별자는 각 연결이 고유하게 식별되어야한다는 것입니다. 이는 연결의 두 끝점에 해당하는 소켓 식별자 쌍을 사용하여 수행됩니다. 여기서 소켓은 단순히 각 프로세스의 IP 주소와 포트 번호의 조합입니다. 즉 소켓 쌍에는 소스 주소, 소스 포트, 대상 주소, 대상 포트의 4가지 정보가 포함됩니다.

VM1에서 캡쳐했던 첫번째 패킷의 connection identifier는

(10.1.1.2: 57488, 10.1.2.2:8080)이고

VM3에서 캡쳐했던 첫번째 패킷의 connection identifier는

(10.1.2.2: 8080, 10.1.1.2:57488)입니다.