8~12장 요약정리

8장\_포트 587번의 정체

SMTP => 메일 전송에 사용되는 전자우편 전송 프로토콜. Simple Mail Transfer Protocol.

TCP 25번 포트를 사용함.

텍스트 기반이고, 모든 문자가 7bit ASCII로 돼 있음.

그 외 경우 : MIME이라는 방식으로 변환돼 전달됨.

포트 587번 : 내부망에서 보안을 위해 SMTP포트 25번을 차단했을 때 쓰는 대체포트.

<SMTP 패킷 분석>

Conversations에서 보면, Port B(목적지 포트)가 587번 포트. 두 번째 세션의 Follow Stream을 보면, 내용 중간부분에 attachment, 그리고 filename = secretrendezvou.docx라는 내용 확인 가능. 파일이 첨부되었음을 알 수 있음.



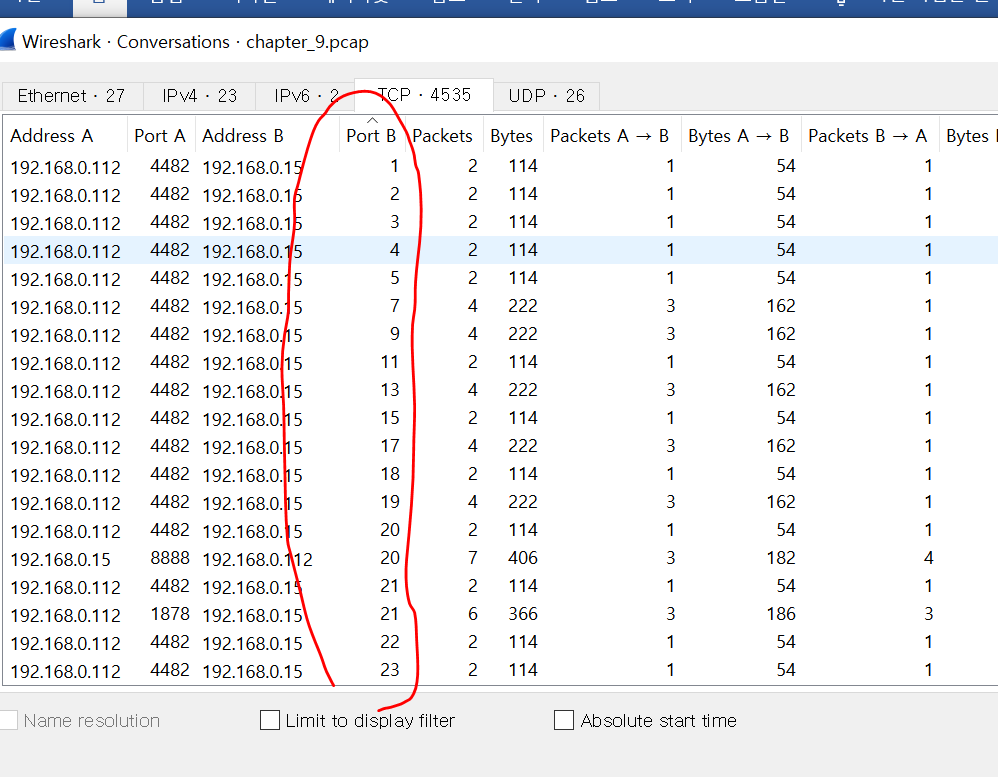
9강\_ 포트스캔 패킷 분석

▣ TCP 스캔 : 3way handshaking을 이용해 포트 오픈여부를 확인하는 기법. (정상적으로 완료 : 오픈o)

▣ UDP : TCP와 달리 3way handshaking 이용 x. 따라서 ICMP unreachable 메시지 회신 여부를 통해 확인함.

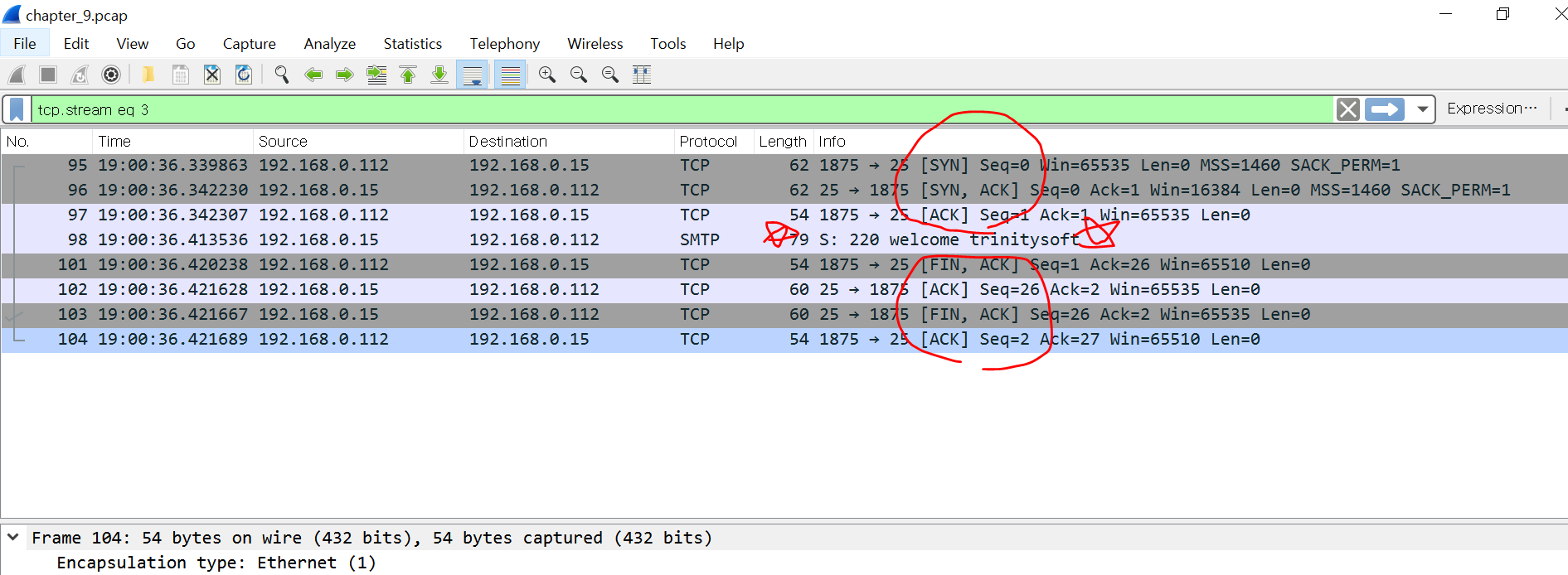
<포트스캔 패킷분석 실습>

Port B 부분을 클릭하면 Conversations의 세션들을 포트번호가 정렬된 상태로 볼 수 있음.



* 확인하려는 포트를 찾기 훨씬 편리함.

포트 25번의 경우를 필터링을 통해 더 자세히 확인해 보면,



세션 연결 이후 즉시 세션 해제 과정이 수행됨.

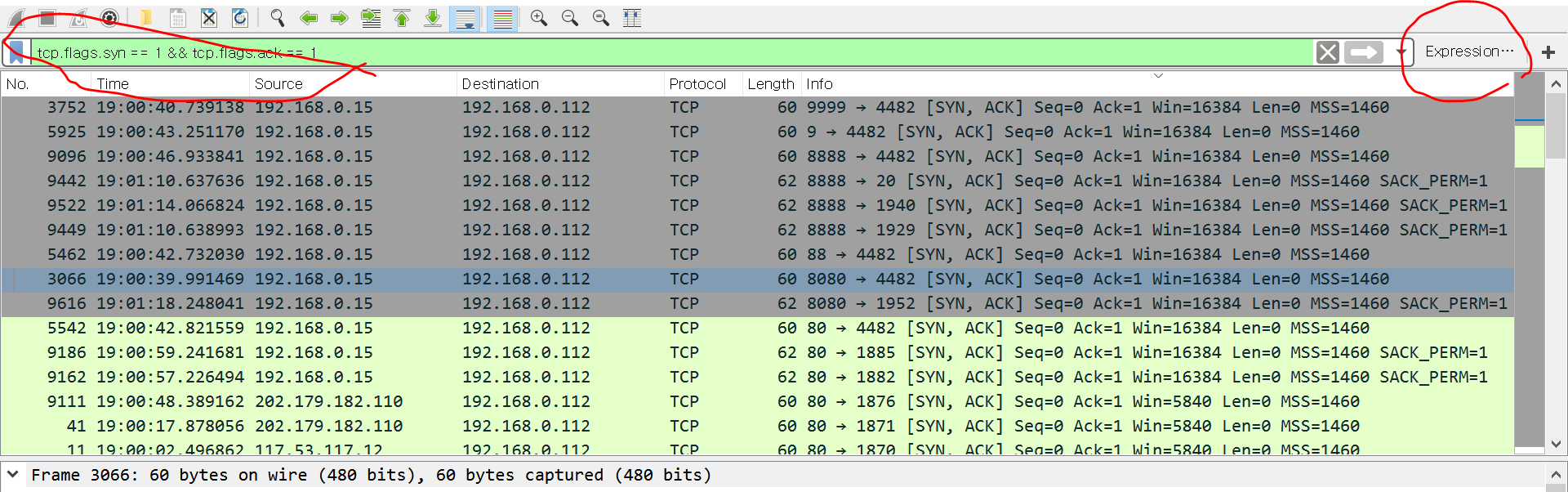
처음 연결 과정에서 25번 포트에서 SYN, ACK으로 회신한 것을 보아 25번 포트가 오픈되어 있음을 확인 할 수 있음.

그 후 바로 세션 해제 과정이 진행된 것을 보아, 단순히 포트스캔을 위한 과정이었음을 알 수 있음.

하지만 포트가 많은 경우 일일이 이러한 과정으로 오픈 여부를 확인하기 힘듦.

* TCP 플래그 정보를 필터링에 적용해서 성공 및 실패 내용만 추출해서 볼 수 있음!

<필터링 이용해서 TCP공격 **성공** 분석하기>



Expression 버튼을 통해 필터를 플래그로 설정할 수 있음.

결과를 보면 [SYN, ACK] 플래그를 회신하는 포트만 볼 수 있다.

\*실패 분석의 경우 필터 설정 : tcp.flags.reset == 1 && tcp.flags.ack == 1

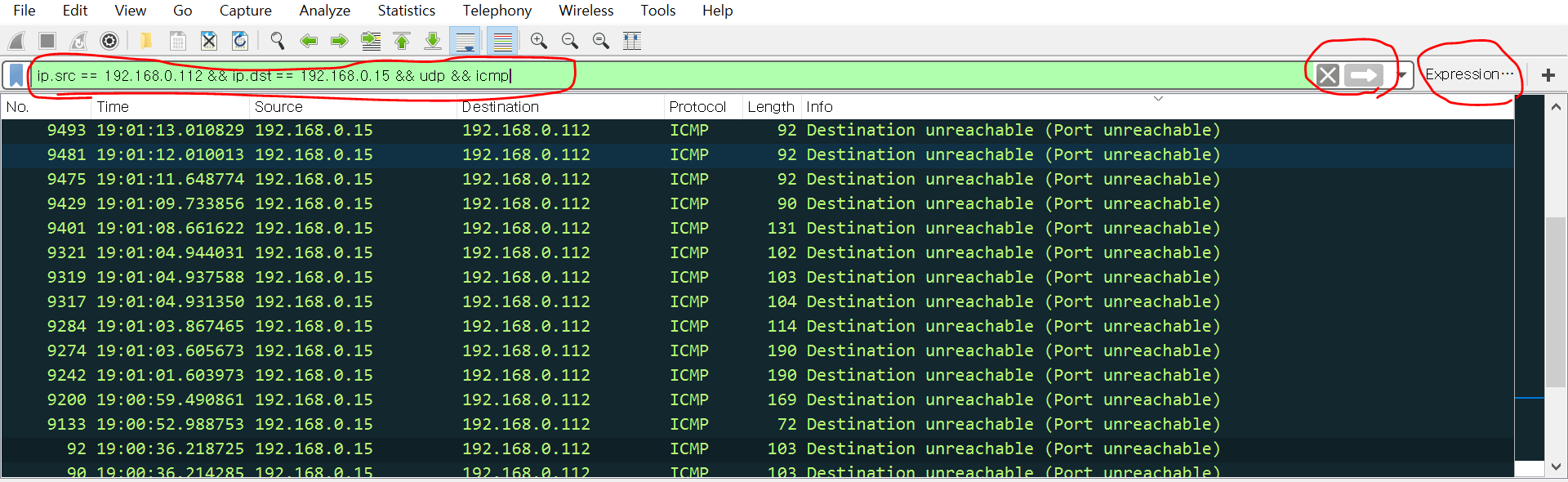
<UDP 공격 실패 추출하기>

\* PCAP 파일에는 여러 IP가 섞여 있어 해당 **접속자와 수신자 IP**만을 필터링해야 함.

\* UDP 프로토콜 상의 공격실패를 추출할 것이므로 **UDP**만을 필터링해야 함.

\* ICMP를 이용한 unreachable 메시지를 회신한 포트가 실패한 포트이므로, **ICMP 프로토콜**만을 필터링 해야 함.

필터 식 : ip.src == 192.168.0.112 && ip.dst == 192.168.0.15 && udp && icmp

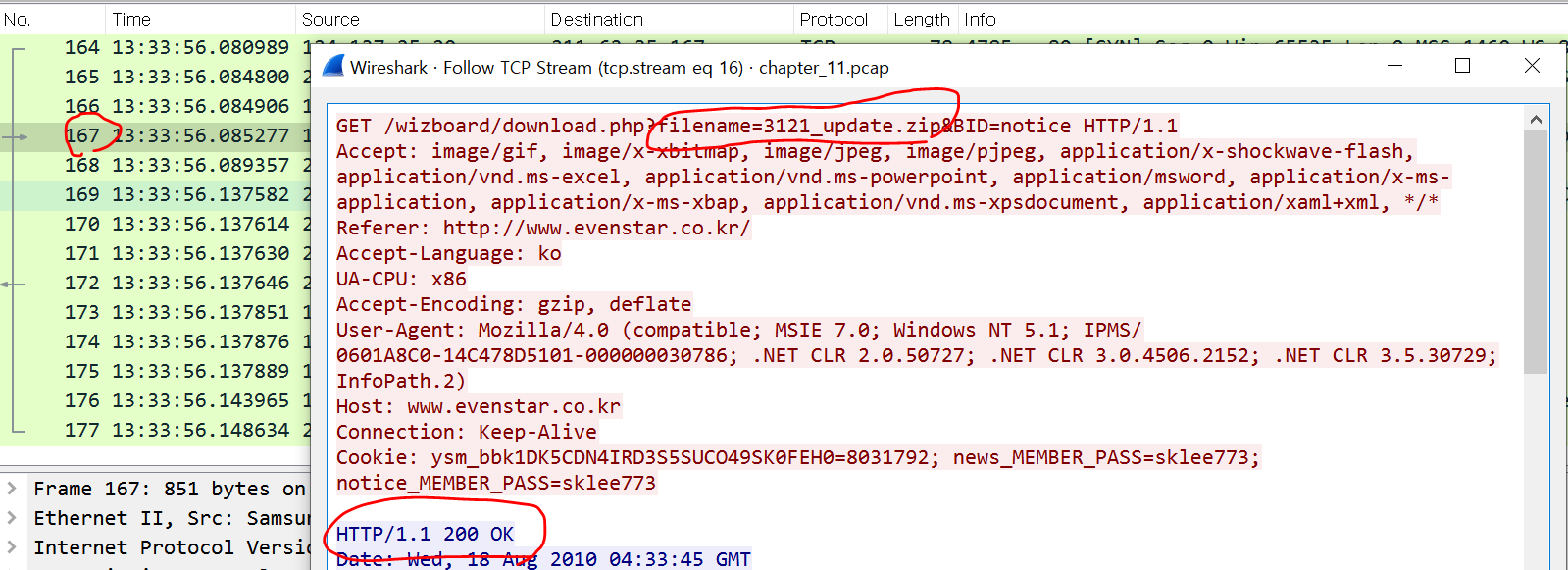


성공사례의 경우 : icmp unreachable 메시지를 회신할 일 없음. 따라서 not icmp를 식에 넣어주면 됨.

식 : ip.src == 192.168.0.112 && ip.dst == 192.168.0.15 && udp && not icmp

11강\_ 백도어 패킷분석

\* 컴퓨터 시스템의 백도어 : 인증을 거친 후 원격접속을 보장하여 시스템에 악의적인 행동을 하는 프로그램.



167번 패킷을 Follow TCP stream으로 확인해 보면 클라이언트가 update.zip 파일을 다운받는 데 성공했음을 알 수 있다. Raw 파일로 저장해서 HexD로 편집해서 추출하면 exe파일을 찾을 수 있다.

\*DLL : Dynamic Link Library

DLL 라이브러리는 암시적 링크(Implicit)와 명시적 링크(Explicit)를 이용해 호출할 있다.

▪ 암시적 링크 : 최초 실행 시 자동으로 해당 라이브러리를 로딩하도록 함.

▪ 명시적 링크 : 필요한 시점에 DLL 파일(라이브러리)을 메모리에 로딩, 파일 내 사용되는 함수 포인터를 직접 검색해 호출하도록 함.