과제 7. SimTL의 ICMP 디코더 모듈 개발

1. 개요

1) 관련 RFC 문서를 읽어본다.
2) SimTL에서 ICMP를 분석하는 모듈, 즉 ICMP 디코더(decoder)를 개발하고, 요약 파일에 관련부분을 추가한다.

2. 수행할 과제 내용

2.1 관련 RFC 문서(직접 찾아서)를 읽고 요약한다(1쪽 정도)

2.2 ICMP 디코더 모듈을 개발하여 SimTL에 추가한다.

1) 요약파일에 프로토콜 유형과 간단한 설명을 기입한다.
2) 감시한 프레임에 대해 다음과 같이 ICMP 메시지를 분석(디코딩)하여 해당 파일에 기입한다. 구체적 디코딩 방법은 관련 RFC 문서와 "5. SMS TM의 ICMP 디코딩 자료"를 참조한다.
   - Type 0(에코응답)은 처음 두 워드, 즉 Type, Code, Checksum, Identifier 및 sequence number만 별도로 보여준다.
   - Type 3(목적지 도달불가)은 처음 1 워드, 즉 Type, Code 및 Checksum만 별도로 보여준다. 목적지 도달 불가의 이유는 매우 중요하므로 반드시 Code를 해석하여 의미를 보여준다. 의미는 관련 RFC문서 찾아볼 것
   - Type 8(에코요청)은 Type 0과 마찬가지로 한다.
   - Type 11(시간초과)는 Type 3과 마찬가지로 한다.
   - 나머지 Type 들은 Type와 Code만 별도로 보여준다.
3) SimTL의 수행 결과를 SMS TM의 결과와 비교하여 제대로 개발되었는지 확인한다. 이때 "4. ICMP 메시지 생성 방법"을 참조하여 모든 메시지 타입에 대해 확인한다.

3. 수행 과제 보고

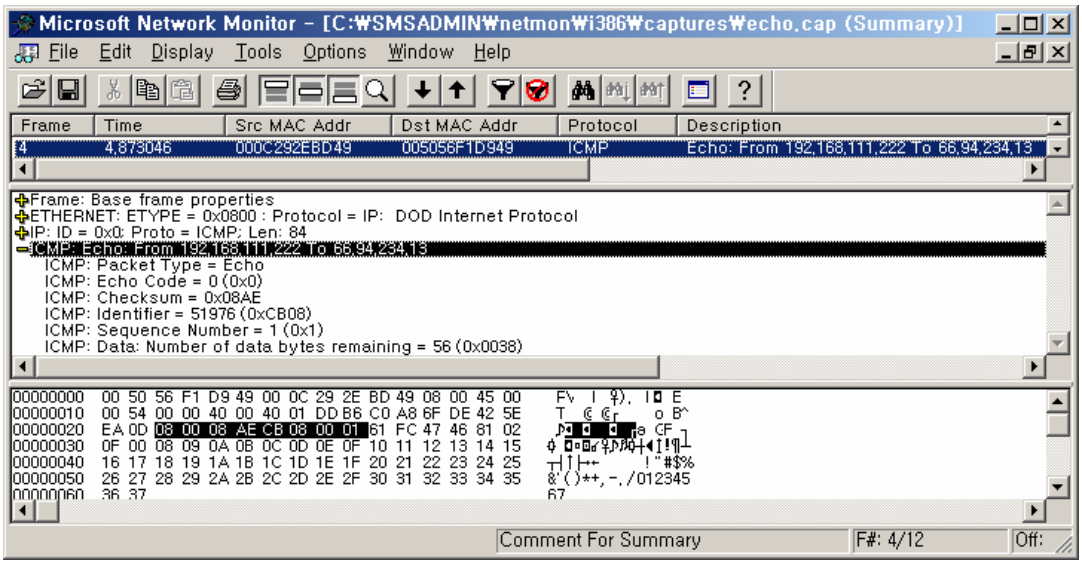
- 과제보고서 작성 및 제출방법 (홈피 자료 참조)에 따라 작성하여 제출할 것
- 덧붙여 추가할 내용
  - 읽은 RFC 문서 요약
  - 완성된 프로그램 일부와 수행 결과 예 (화면 캡쳐할 것)
- 인용처(**막연한 학우 대신 구체적 이름**)와 인용내역을 상세히 기술할 것

4. ICMP 메시지 생성방법

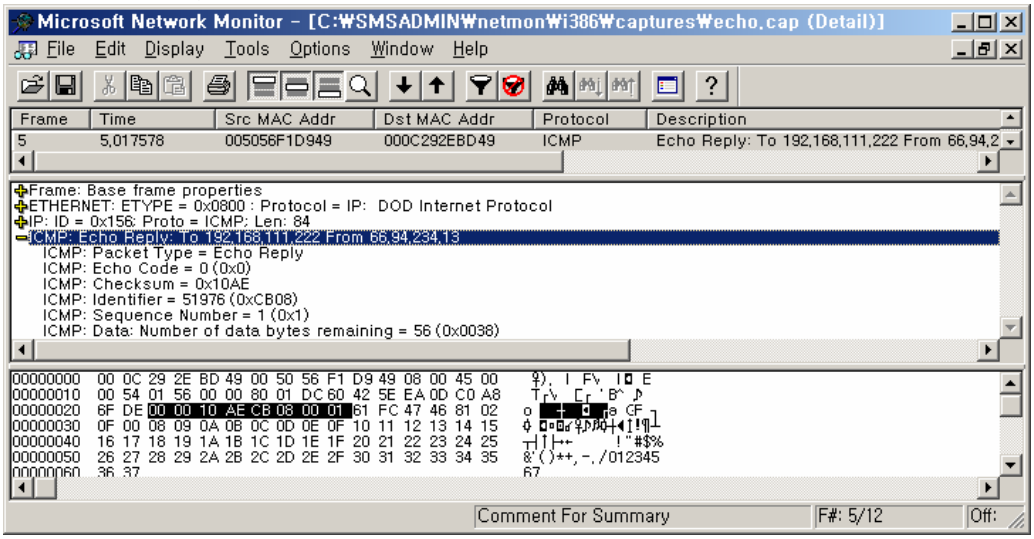
1) Type 0(에코응답)과 Type 8(에코요청)은 ping 시험으로 생성한다.
2) Type 11(시간초과)는 리눅스에서 “tracert yahoo.com” 명령어 수행으로 생성한다. Tracert는 에코요청을 보낸 후 시간초과 메시지를 받는 형태이므로 적어도 2개 이상 캡춰해야 잡을 수 있음.
3) Type 3(목적지 도달불가)의 생성은 패킷을 보낼 수 없도록 해야 하므로 다소 복잡하며, 구체적으로 다음과 같음
   - XP의 명령창에서 “route print”하여 default gateway 레코드를 살펴본다.
   - “route delete 0.0.0.0” 명령어를 입력하여 default gateway를 삭제한다.
   - 리눅스에서 ping yahoo.com 한다
   - 이제 XP에서 default gateway를 모르기 때문에 에코요청 메시지를 보낼 수 없어서 목적지 도달불가 ICMP 메시지를 생성하여 발신측에 응답하게 된다.
   - 참고로 XP는 더 이상 외부와 통신이 안되므로 route add 명령어로 default gateway를 추가하던지, 컴퓨터를 재 시작하여 복구한다.

5. SMS TM의 ICMP 디코딩 자료

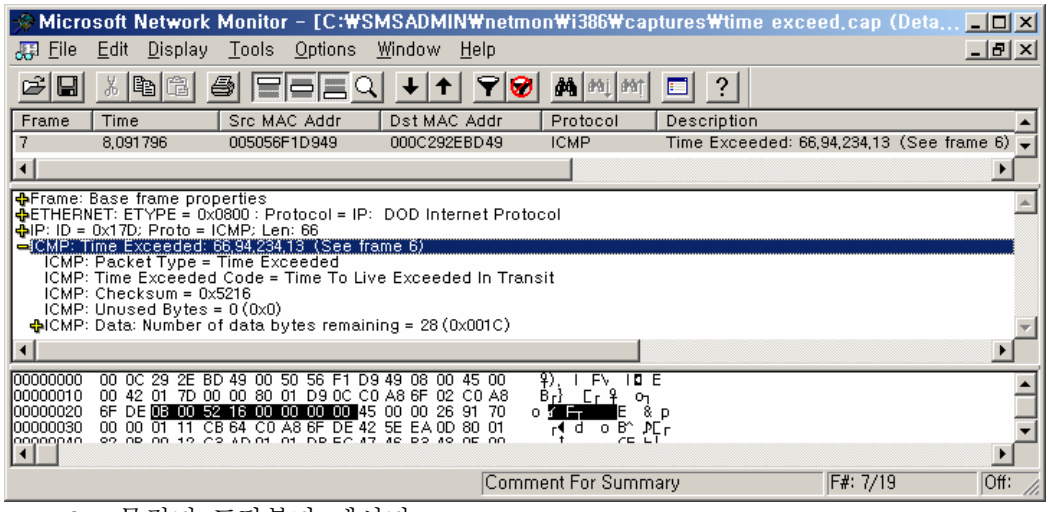
- 에코요청메시지



- 에코응답 메시지



- 시간초과 메시지



- 목적지 도달불가 메시지