과제 3. SimTL 플랫폼 개발

1. 개요

- SimTL은 플랫폼과 개별 프로토콜 분석모듈 (Decoder)들로 구성된다. 플랫폼이란 개별 프로토콜 분석모듈들을 지원하는 공통기능을 갖는 것으로 SimTL의 골격을 이룬다.
- 본 과제에서 SimTL의 플랫폼을 개발하고 검증하여 앞으로 수행할 개별 프로토콜 분석 모듈의 개발을 준비한다.

2. 과제 내용

- 첨부된 개발 요구사항을 참조하여 SimTL 플랫폼을 개발한다.

- 감시한 패킷의 요약부분과 상세내역 부분을 다음과 같이 출력되도록 한다. 참고로 앞으로 새로운 프로토콜 디코더(분석모듈)를 추가할 때 마다 요약부분과 특히 상세내역 부분이 확장될 것임
  - 요약부분에는 프레임 번호와 감시한 시각 정보가 출력되도록 한다.
  - 상세내역 부분에는 코드부분만 출력되도록 한다. 앞으로 프로토콜을 해석하게 되면 해석부분을 추가해야 함.

- 개발된 플랫폼을 리눅스 상에서 수행시켜 실제 패킷을 잡아보고, SMS TM의 수행결과와 비교하여 제대로 개발되었는지 확인 및 검증한다.

3. 과제 보고

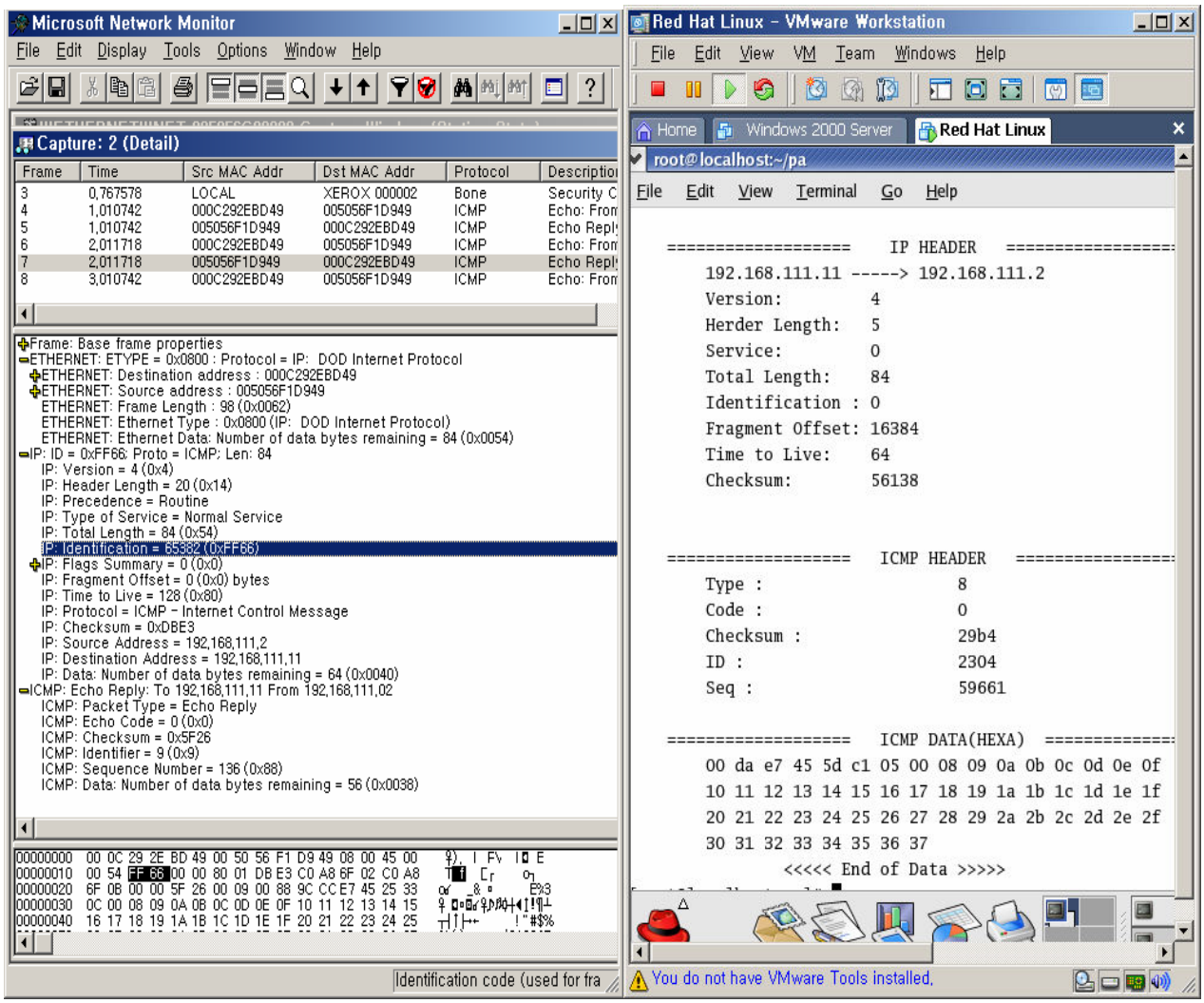
- 반드시 과제보고서 작성 및 제출방법 (홈피 자료 참조)에 따라 작성하여 제출할 것
- 추가적으로 포함시킬 내용
  A. 설계한 플랫폼의 순서도 (한.두쪽 정도)
  B. 프로그램과 수행 결과 예 (수행결과는 화면 캡쳐할 것)
  C. 기타

첨부: 간이형 트래픽 분석기(SimTL) 개발 요구사항

1. 개요

- 제공된 예제 프로그램은 패킷의 분석결과를 하나의 화면에 보여주기 때문에 사용하기 불편함.
- 따라서 상용 트래픽 분석기인 SMS TM(Traffic Monitor)의 출력형식을 모방하여 보다 판독과 분석이 용이하도록 개선하고자 함.
  - SMS TM은 3개의 창으로 결과를 보여주며, 원할 경우 결과를 파일로 저장할 수 있음
  - Summary 창, Decode 창 및 Encode 창

- 참고: 결과출력 비교 (왼쪽이 SMS TM 출력화면, 오른쪽이 샘플 프로그램 출력화면)



2. 개발 요구사항

2.1 개요

1) 감시한 패킷들에 대한 분석 결과를 요약정보를 갖는 Summary(요약)와 상세한 정보를 갖는 Details(상세내역)의 두 부분으로 나누어 취급한다.

2) 감시한 패킷들에 대한 분석 결과는 임시 디렉토리내 임시 파일로 저장하고, 사용자의 요구시 원하는 곳에 원하는 이름으로 저장할 수 있도록 한다.

2.1 요약 부분에 대한 사항

3) 감시한 프레임들의 요약내용을 SMS TM의 Summary 창과 같이 간략히 화면에 나열하고 동시에 임시파일에 저장한다. 여기서 나열되는 줄을 레코드, 줄에 포함되는 정보를 필드라 한다.

4) 각 레코드는 프레임 번호, 감시한 시각, 프레임을 대략적으로 파악할 수 있는 정보 등의 필드를 포함해야 한다.

2.2 상세내역 부분에 대한 사항

5) 프레임에 대한 상세한 분석내용을 갖는 것으로 요약 부분의 프레임 번호를 파일명으로 임시 디렉토리에 저장한다. 감시한 프레임이 n개이면 n개의 파일이 생성된다.

6) 상세내역은 해석(Decode)과 코드(Encode)의 두 부분으로 구성한다.

7) 해석(Decode)부분은 "프로토콜명: Len=XX, Head= 1X 6X."로 해당 프로토콜 부분을 요약한 후 다음 줄에 상세한 해석결과를 수록한다.

* 예를 들면 다음과 같다.

Ethernet: Len= xx, Head=03 6X 4X….
    상세한 해석결과
IP: Len = yy, Head= 04 7X…
    상세한 해석결과
ICMP: Len = yy, Head= 04 7X…
  상세한 해석결과

8) 코드(Encode)부분은 프레임 전체의 이진코드와 ASCII 문자열을 보여주는 것으로 한 줄에 16바이트(또는 32바이트)씩 Hex-Decimal코드와 대응 ASCII 문자열을 나열한다. 참고로 line feed와 carriage return 문자에 해당하는 코드를 제거하지 않으면 ASCII 문자열 부분이 깨어져 보임.

2.3 기타

9) tcpdump에서 지원하는 필터링 규칙(primitive)을 수용하여야 한다 (예제 프로그램에 이미 포함되어 있음)

10) 최대 감시 패킷의 수를 MAX_PACKETS로 제한한다(기본값 1000개).

11) 더 좋은 아이디어가 있으면 요구사항을 수정할 수 있다.