과제 03 수행보고서

정보통신공학전공

200301582
김성태

ubuntu

수행 목적

- 1. SimTL 플랫폼 개발
  - SimTL 은 플랫폼과 개별 프로토콜 분석모듈 (Decoder) 들로 구성된다 . 플랫폼이란 개별 프로토콜 분석모듈들을 지원하는 공통기능을 갖는 것으로 SimTL 의 골격을 이룬다 .
- 2. SimTL 분석 모듈 개발 준비
  - SimTL 의 플랫폼을 개발하고 검증하여 앞으로 수행할 개별 프로토콜 분석 모듈의 개발을 준비한다 .

개발 요구 사항 1

- Summary(요약), Details (상세내역) 으로 구분
- Summary(요약)
  - 감시한 패킷들에 대한 분석 결과에 대한 요약정보를 갖는다 .
- Details(상세내역)
  - 패킷 내용에 대해 상세한 정보를 갖는다 .
- 분석 결과는 임시 디렉토리내 임시 파일로 저장
- 사용자의 요구시 원하는 곳에 원하는 이름으로 저장할 수 있도록 한다 .

개발 요구 사항 2

- 요약 부분
  - 감시한 프레임들의 요약내용을 SMS Tm 의 Summary 창과 같이 간략히 화면에 나열하고 동시에 임시파일에 저장한다. 여기서 나열되는 줄을 레코드, 줄에 포함되는 정보를 필드라 한다.
  - 각 레코드는 프레임 번호, 감시한 시각, 프레임을 대략적으로 파악할 수 있는 정보등의 필드를 포함해야 한다.
- 상세내역 부분
  - 프레임에 대한 상세한 분석내용을 갖는 것으로 요약 부분의 프레임 번호를 파일명으로 임시 디렉토리에 저장한다. 감시한 프레임이 n 개이면 n 개의 파일이 생성된다.
  - 상세내역은 해석 (Decode) 과 코드 (Encode) 의 두 부분으로 구성한다.

ubuntu

프로그램의 구성 1 (파일)

- SimTL_beta.c
  - SimTL 프로그램의 시작부분
- SimTL.h
  - SimTL 의 헤더파일 . 모든 함수의 원형이 선언되어 있다 .
- SimTL.c
  - SimTL 구현의 핵심파일 . 모든 함수의 구현이 들어 있다 .

프로그램의 구성 2(함수)

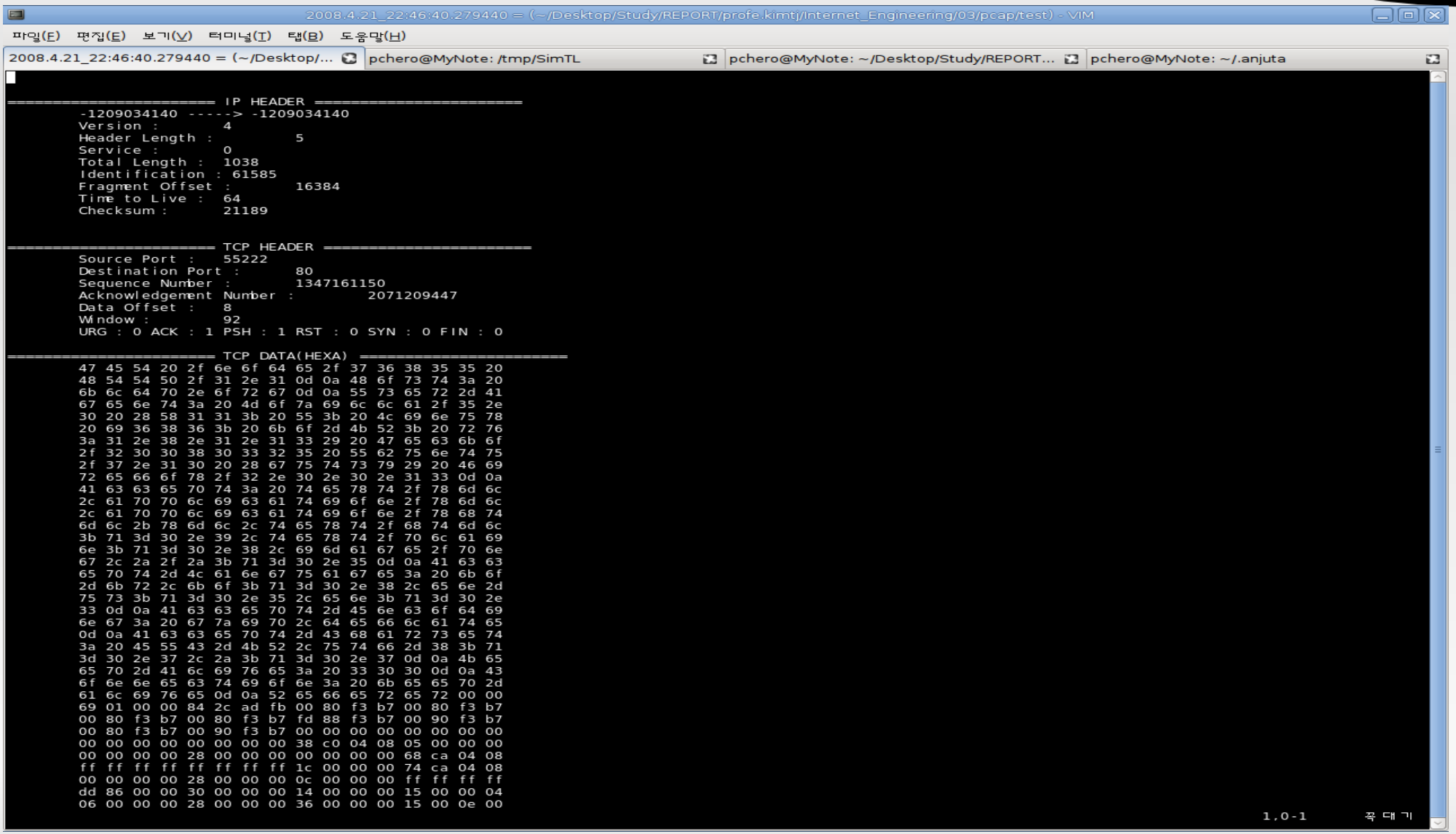
- /* 현재 시각을 기준으로 파일을 만들어 파일 기술자를 리턴 */
  - FILE *make_tmpfile(FILE *fd_dir);
- /* 임시 디렉토리를 만들고 디렉토리 관리 파일을 생성 */
  - void make_tmpdirec(void);
- /* 패킷을 잡는 pcap 함수 */
  - int packet_capture(pcap_option *pcap_option);
- /* 패킷을 분석하는 packet_analysis */
  - void packet_analysis(unsigned char *, const struct pcap_pkthdr *, const unsigned char *);
- /* DataLink Type 에 따라 수행될 함수를 결정하는 lookup_printer */
  - static pcap_handler lookup_printer(int type);
- /* Signal 설정 */
  - void sig_int(int sig);
- /* 사용법 설명 */
  - void usage(void);
- /* 옵션 거르기 */
  - void get_option(char **argv, pcap_option *p_option);
- /* 저장 여부를 물어보고 저장을 시도한다 . */
  - void tmp_save(void);

실행화면 - 요약 & 파일저장

```
pchero@MyNote: ~/Desktop/Study/REPORT/profe.kimtj/Internet_Engineering/03/pcap/test
파일(F)  편집(E)  보기(V)  터미널(T)  탭(B)  도움말(H)
pchero@MyNote: ~/Desktop/Study/REPORT... | pchero@MyNote: /tmp/SimTL | pchero@MyNote: ~/Desktop/Study/REPORT... | pchero@MyNote: ~/.anjuta
2008.4.21_22:46:40.279440  2008.4.21_22:46:40.591115  2008.4.21_22:46:40.600959  2008.4.21_22:46:40.696834  2008.4.21_22:46:40.697202
2008.4.21_22:46:40.572857  2008.4.21_22:46:40.591239  2008.4.21_22:46:40.696500  2008.4.21_22:46:40.696927  2008.4.21_22:46:40.697293
pchero@MyNote:~/Desktop/Study/REPORT/profe.kimtj/Internet_Engineering/03/pcap/test$ cd ..
pchero@MyNote:~/Desktop/Study/REPORT/profe.kimtj/Internet_Engineering/03/pcap$ ls
SimTL.c  SimTL.h  SimTL.o  main  main.c  main.o  test
pchero@MyNote:~/Desktop/Study/REPORT/profe.kimtj/Internet_Engineering/03/pcap$ ./main
 Usage : pa filter_rule [-pch]
         -p   :  데이타를 문자로 출력한다.
         -c   :  주어진 숫자만큼의 패킷만 덤프한다
          -e  :  datalink layer를 출력한다.
          -e  :  잡은 패킷을 생으로 찍는다.
         -h   :  사용법
pchero@MyNote:~/Desktop/Study/REPORT/profe.kimtj/Internet_Engineering/03/pcap$ ./main
bash: ./main: No such file or directory
pchero@MyNote:~/Desktop/Study/REPORT/profe.kimtj/Internet_Engineering/03/pcap$ ./SimTL_beta
 Usage : SimTL_beta filter_rule [-pch]
         -p   :  데이타를 문자로 출력한다.
         -c   :  주어진 숫자만큼의 패킷만 덤프한다
          -e  :  datalink layer를 출력한다.
          -e  :  잡은 패킷을 생으로 찍는다.
         -h   :  사용법
pchero@MyNote:~/Desktop/Study/REPORT/profe.kimtj/Internet_Engineering/03/pcap$ sudo ./SimTL_beta "src host 192.168.10.110 and tcp port 80" -i eth0 -e -p -c 2
0 -r
[sudo] password for pchero:
device = eth0
0: /tmp/SimTL/2008.4.21_23:43:2.459579  IP->    -1208456604----->-1208456604 Version:4 Header_Length:5 Service:0 Total_Length:60
1: /tmp/SimTL/2008.4.21_23:43:2.465598  IP->    -1208456604----->-1208456604 Version:4 Header_Length:5 Service:0 Total_Length:52
2: /tmp/SimTL/2008.4.21_23:43:2.465901  IP->    -1208456604----->-1208456604 Version:4 Header_Length:5 Service:0 Total_Length:880
3: /tmp/SimTL/2008.4.21_23:43:2.514859  IP->    -1208456604----->-1208456604 Version:4 Header_Length:5 Service:0 Total_Length:52
4: /tmp/SimTL/2008.4.21_23:43:3.320380  IP->    -1208456604----->-1208456604 Version:4 Header_Length:5 Service:0 Total_Length:880
5: /tmp/SimTL/2008.4.21_23:43:3.362611  IP->    -1208456604----->-1208456604 Version:4 Header_Length:5 Service:0 Total_Length:52
6: /tmp/SimTL/2008.4.21_23:43:4.131115  IP->    -1208456604----->-1208456604 Version:4 Header_Length:5 Service:0 Total_Length:880
7: /tmp/SimTL/2008.4.21_23:43:4.138219  IP->    -1208456604----->-1208456604 Version:4 Header_Length:5 Service:0 Total_Length:52
8: /tmp/SimTL/2008.4.21_23:43:5.226404  IP->    -1208456604----->-1208456604 Version:4 Header_Length:5 Service:0 Total_Length:880
9: /tmp/SimTL/2008.4.21_23:43:5.233493  IP->    -1208456604----->-1208456604 Version:4 Header_Length:5 Service:0 Total_Length:52
10: /tmp/SimTL/2008.4.21_23:43:6.34268  IP->    -1208456604----->-1208456604 Version:4 Header_Length:5 Service:0 Total_Length:880
11: /tmp/SimTL/2008.4.21_23:43:6.41337  IP->    -1208456604----->-1208456604 Version:4 Header_Length:5 Service:0 Total_Length:52
12: /tmp/SimTL/2008.4.21_23:43:6.825959  IP->    -1208456604----->-1208456604 Version:4 Header_Length:5 Service:0 Total_Length:880
13: /tmp/SimTL/2008.4.21_23:43:6.833057  IP->    -1208456604----->-1208456604 Version:4 Header_Length:5 Service:0 Total_Length:52
14: /tmp/SimTL/2008.4.21_23:43:7.562933  IP->    -1208456604----->-1208456604 Version:4 Header_Length:5 Service:0 Total_Length:880
15: /tmp/SimTL/2008.4.21_23:43:7.570080  IP->    -1208456604----->-1208456604 Version:4 Header_Length:5 Service:0 Total_Length:52
16: /tmp/SimTL/2008.4.21_23:43:8.272638  IP->    -1208456604----->-1208456604 Version:4 Header_Length:5 Service:0 Total_Length:880
17: /tmp/SimTL/2008.4.21_23:43:8.279806  IP->    -1208456604----->-1208456604 Version:4 Header_Length:5 Service:0 Total_Length:52
18: /tmp/SimTL/2008.4.21_23:43:9.18427  IP->    -1208456604----->-1208456604 Version:4 Header_Length:5 Service:0 Total_Length:880
19: /tmp/SimTL/2008.4.21_23:43:9.25517  IP->    -1208456604----->-1208456604 Version:4 Header_Length:5 Service:0 Total_Length:52
Do you want a Save? [Y/n] :y
Type the save path.
Dir : ./test
/bin/cp -f /tmp/SimTL/* ./testpchero@MyNote:~/Desktop/Study/REPORT/profe.kimtj/Internet_Engineering/03/pcap$ ls
SimTL.c  SimTL.h  SimTL.o  SimTL_beta  SimTL_beta.c  SimTL_beta.o  main.c  main.o  test
pchero@MyNote:~/Desktop/Study/REPORT/profe.kimtj/Internet_Engineering/03/pcap$ cd test/
pchero@MyNote:~/Desktop/Study/REPORT/profe.kimtj/Internet_Engineering/03/pcap/test$ ls
2008.4.21_22:46:40.270865  2008.4.21_22:46:40.599885  2008.4.21_22:46:40.697202  2008.4.21_23:43:4.138219  2008.4.21_23:43:8.272638
2008.4.21_22:46:40.279112  2008.4.21_22:46:40.600959  2008.4.21_22:46:40.697293  2008.4.21_23:43:5.226404  2008.4.21_23:43:8.279806
2008.4.21_22:46:40.279440  2008.4.21_22:46:40.696500  2008.4.21_23:43:2.459579   2008.4.21_23:43:5.233493  2008.4.21_23:43:9.18427
2008.4.21_22:46:40.572857  2008.4.21_22:46:40.696647  2008.4.21_23:43:2.465598   2008.4.21_23:43:6.34268   2008.4.21_23:43:9.25517
2008.4.21_22:46:40.573811  2008.4.21_22:46:40.696742  2008.4.21_23:43:2.465901   2008.4.21_23:43:6.41337   traceManager
2008.4.21_22:46:40.590826  2008.4.21_22:46:40.696834  2008.4.21_23:43:2.514859   2008.4.21_23:43:6.825959
2008.4.21_22:46:40.591115  2008.4.21_22:46:40.696927  2008.4.21_23:43:3.320380   2008.4.21_23:43:6.833057
2008.4.21_22:46:40.591239  2008.4.21_22:46:40.697018  2008.4.21_23:43:3.362611   2008.4.21_23:43:7.562933
2008.4.21_22:46:40.591355  2008.4.21_22:46:40.697109  2008.4.21_23:43:4.131115   2008.4.21_23:43:7.570080
pchero@MyNote:~/Desktop/Study/REPORT/profe.kimtj/Internet_Engineering/03/pcap/test$
```

ubuntu

실행화면 - 상세


2008.4.21_22:46:40.279440 = (~/Desktop/Study/REPORT/profe.kimtj/Internet_Engineering/03/pcap/test) - VIM
파일(F) 편집(E) 보기(V) 터미널(T) 탭(B) 도움말(H)
2008.4.21_22:46:40.279440 = (~/Desktop/...
pchero@MyNote: /tmp/SimTL
pchero@MyNote: ~/Desktop/Study/REPORT...
pchero@MyNote: ~/.anjuta
========== IP HEADER ==========
-1209034140 -----> -1209034140
Version : 4
Header Length : 5
Service : 0
Total Length : 1038
Identification : 61585
Fragment Offset : 16384
Time to Live : 64
Checksum : 21189
========== TCP HEADER ==========
Source Port : 55222
Destination Port : 80
Sequence Number : 1347161150
Acknowledgement Number : 2071209447
Data Offset : 8
Window : 92
URG : 0 ACK : 1 PSH : 1 RST : 0 SYN : 0 FIN : 0
========== TCP DATA(HEXA) ==========
47 45 54 20 2f 6e 6f 64 65 2f 37 36 38 35 35 20
48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20
6b 6c 64 70 2e 6f 72 67 0d 0a 55 73 65 72 2d 41
67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e
30 20 28 58 31 31 3b 20 55 3b 20 4c 69 6e 75 78
20 69 36 38 36 3b 20 6b 6f 2d 4b 52 3b 20 72 76
3a 31 2e 38 2e 31 2e 31 33 29 20 47 65 63 6b 6f
2f 32 30 30 38 30 33 32 35 20 55 62 75 6e 74 75
2f 37 2e 31 30 20 28 67 75 74 73 79 29 20 46 69
72 65 66 6f 78 2f 32 2e 30 2e 30 2e 31 33 0d 0a
41 63 63 65 70 74 3a 20 74 65 78 74 2f 78 6d 6c
2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c
2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74
6d 6c 2b 78 6d 6c 2c 74 65 78 74 2f 68 74 6d 6c
3b 71 3d 30 2e 39 2c 74 65 78 74 2f 70 6c 61 69
6e 3b 71 3d 30 2e 38 2c 69 6d 61 67 65 2f 70 6e
67 2c 2a 2f 2a 3b 71 3d 30 2e 35 0d 0a 41 63 63
65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 6b 6f
2d 6b 72 2c 6b 6f 3b 71 3d 30 2e 38 2c 65 6e 2d
75 73 3b 71 3d 30 2e 35 2c 65 6e 3b 71 3d 30 2e
33 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69
6e 67 3a 20 67 7a 69 70 2c 64 65 66 6c 61 74 65
0d 0a 41 63 63 65 70 74 2d 43 68 61 72 73 65 74
3a 20 45 55 43 2d 4b 52 2c 75 74 66 2d 38 3b 71
3d 30 2e 37 2c 2a 3b 71 3d 30 2e 37 0d 0a 4b 65
65 70 2d 41 6c 69 76 65 3a 20 33 30 30 0d 0a 43
6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d
61 6c 69 76 65 0d 0a 52 65 66 65 72 65 72 00 00
69 01 00 00 84 2c ad fb 00 80 f3 b7 00 80 f3 b7
00 80 f3 b7 00 80 f3 b7 fd 88 f3 b7 00 90 f3 b7
00 80 f3 b7 00 90 f3 b7 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 38 c0 04 08 05 00 00 00
00 00 00 00 28 00 00 00 00 00 00 00 68 ca 04 08
ff ff ff ff ff ff ff ff 1c 00 00 00 74 ca 04 08
00 00 00 00 28 00 00 00 0c 00 00 00 ff ff ff ff
dd 86 00 00 30 00 00 00 14 00 00 00 15 00 00 04
06 00 00 00 28 00 00 00 36 00 00 00 15 00 0e 00
1,0-1
꼭 대 기

참고

- http://www.kldp.org
  - 한국 리눅스 문서 프로젝트
- http://kldp.org/KoreanDoc/Libpcap-KLDP
  - KLDP pcap library 위키
- http://blog.naver.com/jw0502?Redirect=Log&logNo=140049554219
  - 아스키 코드에 대한 자세한 설명이 있는곳
- 리눅스 프로그래밍 – Neil Matthew
- 유닉스 시스템 & 네트워크 프로그래밍 – 신재호

끝

ubuntu