[솔루션 기능 테스트]
리눅스 PC보안용 LAV 테스트
(부요 데스크탑) 기능 테스트 절차서

한국소프트웨어진흥원
공개SW기술지원센터

<Revision 정보>

일자	VERSION	변경내역	작성자
2007. 6.14	0.1	초기 작성	양선주
2007. 6.15	0.2	기능 테스트 중 실시간 감시 테스트 추가	양선주
2007. 6.18	0.3	기능 테스트 중 수동검사 및 비검사 영역 테스트 추가	양선주
2007. 6.19	0.4	기능 테스트 중 검역소/로그보기/업데이트 테스트 추가	양선주

목 차

1. 문서 개요

본 문서는 리눅스 PC보안용 솔루션인 LAV를 Booyo Desktop 2.0 OS(kernel 2.6.15-1)에서 호환성 및 기능성 검증을 중심으로 테스트 하였으며, 관련 솔루션 업체의 참고자료 활용을 위해 제작되었다.

가. 문서의 목적

다음과 같은 세부적인 목적을 달성하기 위하여 작성되었다.

- 리눅스 PC보안 솔루션 LAV와 Booyo Desktop 2.0 OS 호환성 결과
- 리눅스 PC보안 솔루션 LAV와 Booyo Desktop 2.0 OS 기능성 결과
- 진행 중 문제 발생 사항과 각각의 진행사항

나. 본 문서의 사용방법

다음과 같은 방법으로 사용할 수 있다.

- 리눅스 PC보안 솔루션 LAV와 Booyo Desktop 2.0 OS의 기능성 결과를 확인한다.
- Booyo Desktop 2.0 OS에서 LAV의 설치, 구동 및 기능 실행 결과를 확인한다.

2. 테스트 절차 내역

가. LAV 기동 테스트

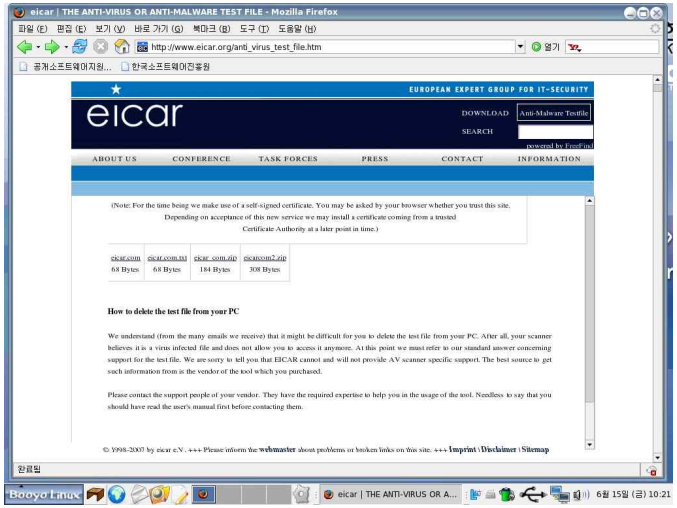
단계	항목/시험/결과	
시험절차	시험항목	LAV 기동 확인
	1	1. X-windows로 로그인 2. 시작메뉴의 프로그램 실행바를 이용하여 실행 3. 기동 확인
시험결과	1	1. X-windows로 로그인 후, 시작메뉴의 프로그램 실행바를 이용하여 실행한다.  2. 가동되는 것을 확인한다. 
비 고		

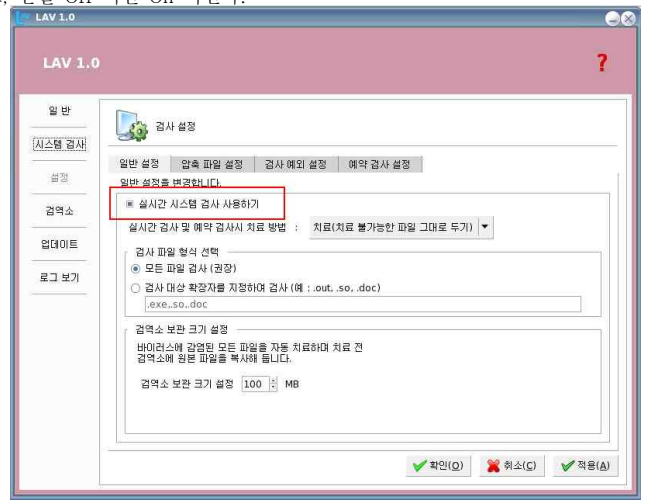
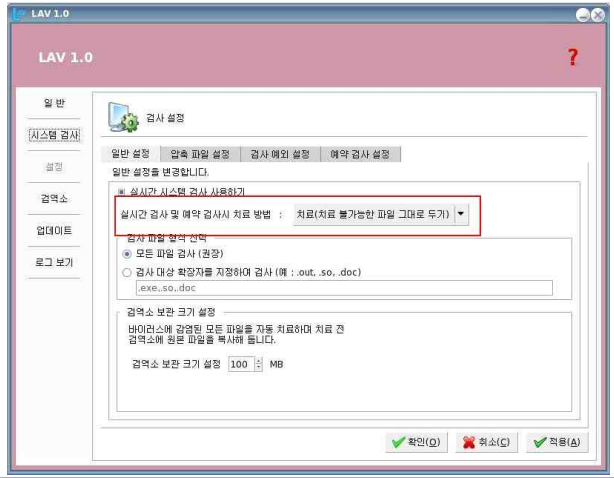
나. LAV 기능 테스트

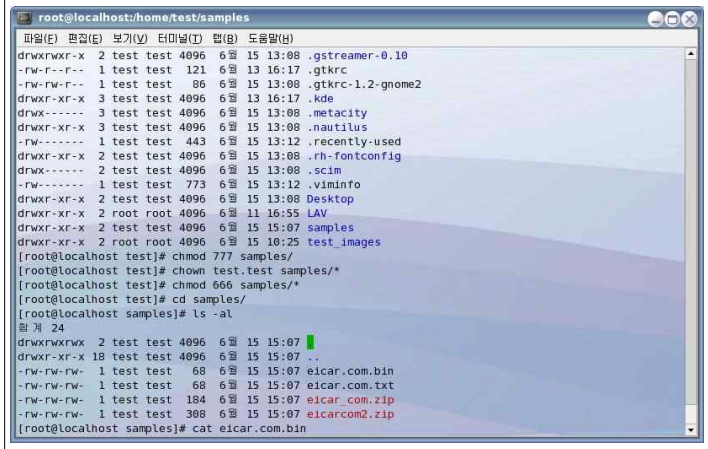
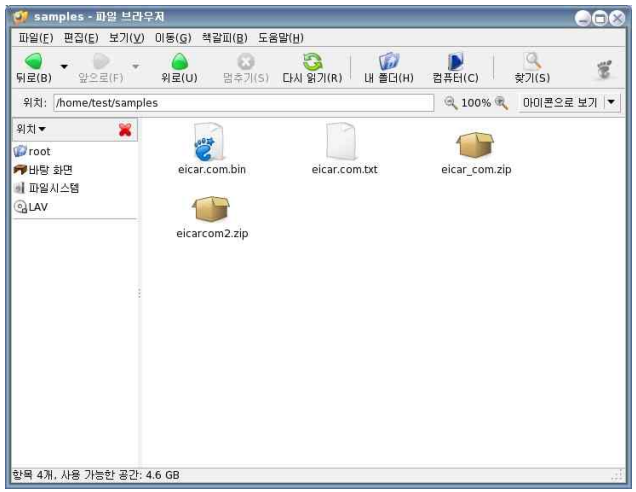
단계	항목/시험/결과	
시험절차	시험항목	LAV의 실시간 검사
	1	1. http://www.eicar.org/anti_virus_test_file.htm 에서 바이러스 샘플파일을 다운로드 하여 해당 시스템에 저장한다. 2. [일반설정] 메뉴에서 '실시간 시스템 검사 사용하기' 가 On 되어 있는지 확인하고, 만일 Off 이면 On 시킨다. 3. 실시간 검사 및 예약 검사시 치료 방법은 [그대로 두기]로 설정한다.
	2	1. 상기의 URL에서 다운로드한 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 일반 사용자로 변경하고, 파일 퍼미션은 666으로 수정한 후, 디렉토리는 777로 변경한다. 2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인한다. 3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인한다. 4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.
	3	1. 상기의 URL에서 다운로드한 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 일반 사용자로 변경하고, 파일 퍼미션은 444로 수정한 후, 디렉토리는 777로 변경한다. 2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인한다. 3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인한다. 4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.
	4	1. 상기의 URL에서 다운로드한 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 root로 변경하고, 파일 퍼미션은 444로 수정한 후, 디렉토리는 777로 변경한다. 2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인한다. 3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인한다. 4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.
	5	1. 상기의 URL에서 다운로드한 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 root로 변경하고, 파일 퍼미션은 444로 수정한 후, 디렉토리는 555로 변경한다. 2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인한다. 3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인한다. 4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.

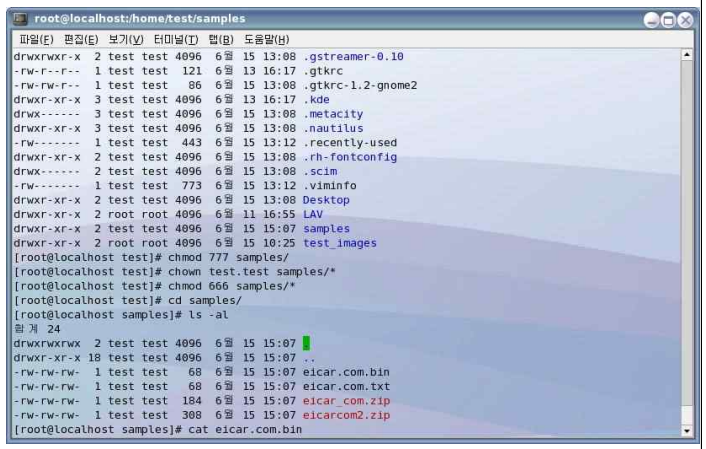
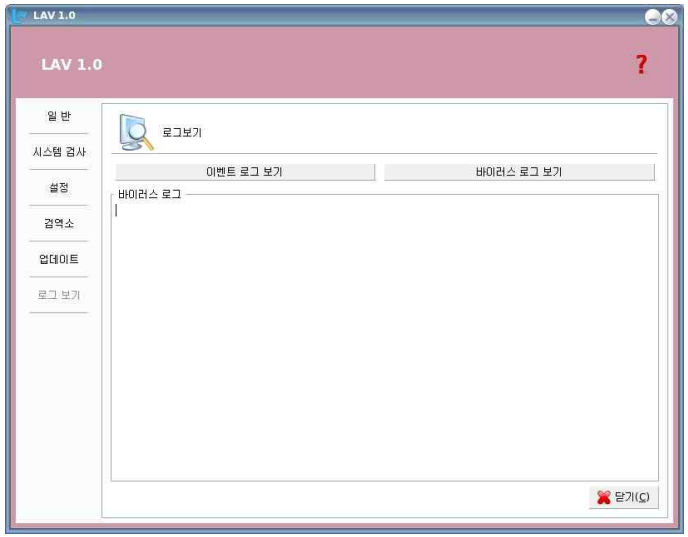
단계	항목/시험/결과	
시험절차	6	1. 상기의 URL에서 다운로드한 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 일반 사용자로 변경하고, 파일과 디렉토리 퍼미션을 777로 수정한다. 2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인한다. 3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인한다. 4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.
	7	1. 상기의 URL에서 다운로드한 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 일반 사용자로 변경하고, 파일 퍼미션은 555, 디렉토리 퍼미션은 777로 수정한다. 2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인한다. 3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인한다. 4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.
	8	1. 상기의 URL에서 다운로드한 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 root로 변경하고, 파일 퍼미션은 555, 디렉토리 퍼미션은 777로 수정한다. 2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인한다. 3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인한다. 4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.
	9	1. 상기의 URL에서 다운로드한 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 root로 변경하고, 파일 퍼미션과 디렉토리 퍼미션을 555로 수정한다. 2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인한다. 3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인한다. 4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.
	10	1. 바이러스 파일을 저장한 CD 매체를 삽입하고 CD 드라이브의 해당 파일을 열어, 접근이 가능한지 확인한다. 2. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인한다. 3. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.
	11	1. [설정] 메뉴에서 '실시간 시스템 검사 사용하기' 가 On 되어 있는지 확인하고, 만일 Off 이면 On 시킨다. 2. 실시간 검사 및 예약 검사시 치료 방법은 [치료(치료 불가능한 파일 삭제)]로 설정한다.

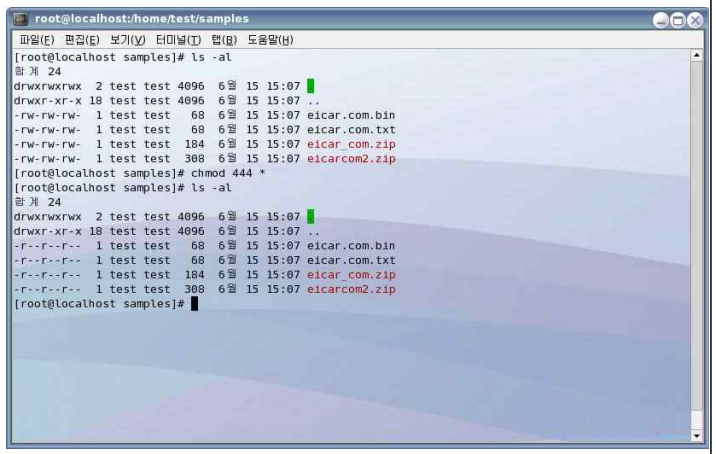
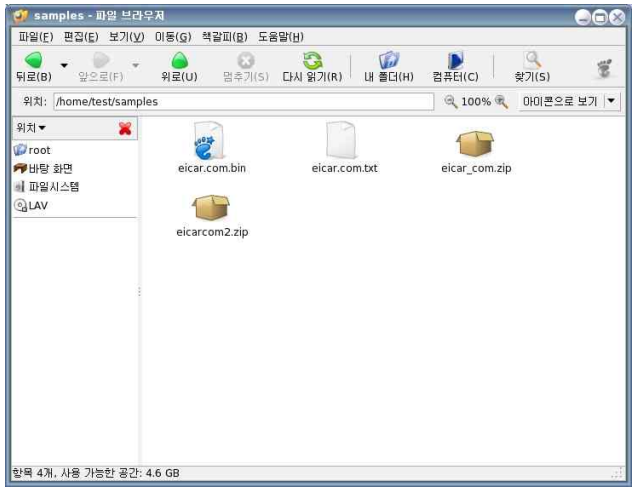
단계	항목/시험/결과	
시험절차	12	1. 바이러스 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 일반 사용자로 변경하고, 파일 퍼미션은 666, 디렉토리 퍼미션은 777로 수정한다. 2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인한다. 3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인한다. 4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.
	13	1. 바이러스 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 일반 사용자로 변경하고, 파일 퍼미션은 444, 디렉토리 퍼미션은 777로 수정한다. 2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인한다. 3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인한다. 4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.
	14	1. 바이러스 파일을 저장한 CD 매체를 삽입하고 CD 드라이브의 해당 파일을 열어, 접근이 가능한지 확인한다. 2. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인한다. 3. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.
	15	1. 바이러스 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 일반 사용자로 변경하고, 파일과 디렉토리 퍼미션을 777로 수정한다. 2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인한다. 3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인한다. 4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.
	16	1. [설정] 메뉴에서 '실시간 시스템 검사 사용하기' 가 On 되어 있는지 확인하고, 만일 Off 이면 On 시킨다. 2. 실시간 검사 및 예약 검사시 치료 방법은 [치료(치료 불가능한 파일 그대로 두기)]로 설정한다.
	17	1. 바이러스 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 일반 사용자로 변경하고, 파일과 디렉토리 퍼미션을 777로 수정한다. 2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인한다. 3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인한다. 4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.

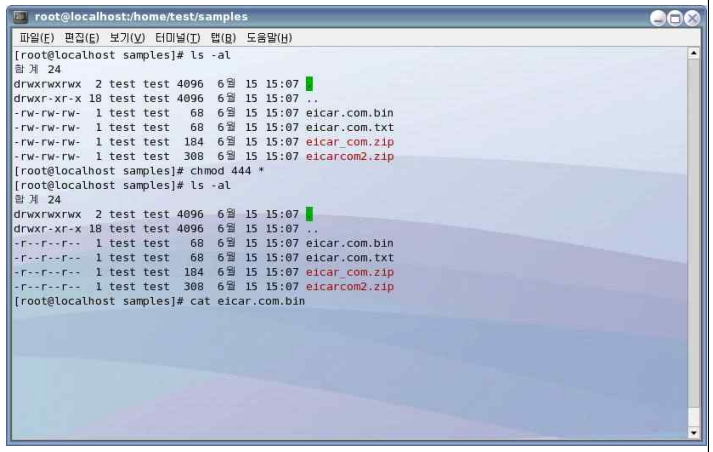
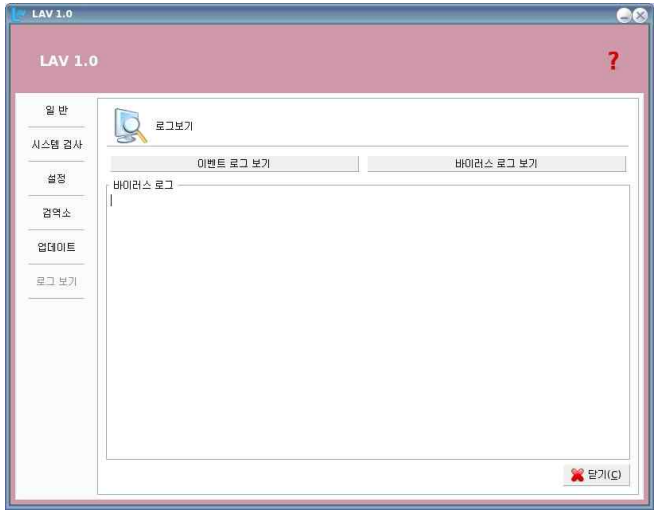
단계	항목/시험/결과	
시험절차	18	1. 바이러스 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 일반 사용자로 변경하고, 파일의 퍼미션을 555로, 디렉토리 퍼미션을 777로 수정한다. 2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인한다. 3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인한다. 4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.
	19	1. 바이러스 파일을 저장한 CD 매체를 삽입하고 CD 드라이브의 해당 파일을 열어, 접근이 가능한지 확인한다. 2. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인한다. 3. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.
시험결과	1	1. http://www.eicar.org/anti_virus_test_file.htm에서 바이러스 샘플파일 다운로드 

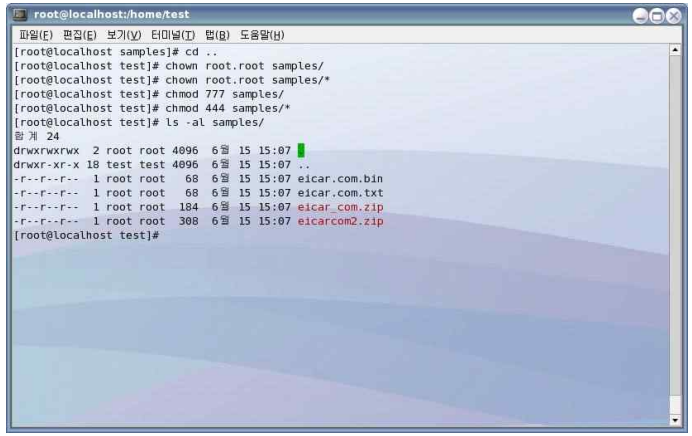
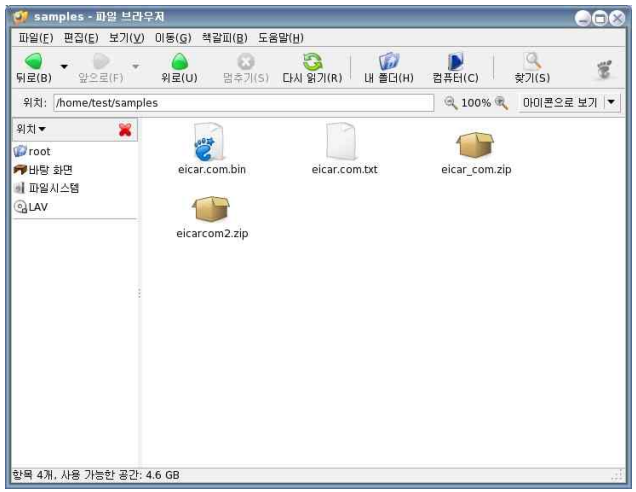
단계	항목/시험/결과	
시험결과	1	2. [설정] 메뉴에서 '실시간 시스템 검사 사용하기' 가 On 되어 있는지 확인하고, 만일 Off 이면 On 시킨다.  3. 실시간 검사 및 예약 검사시 치료 방법은 [그대로 두기]로 설정한다. 

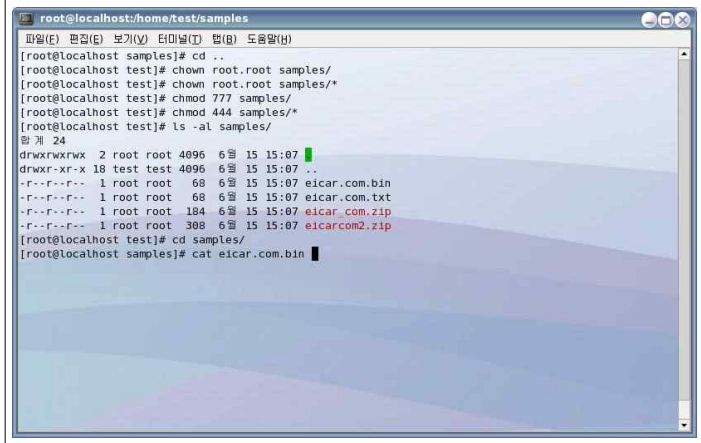
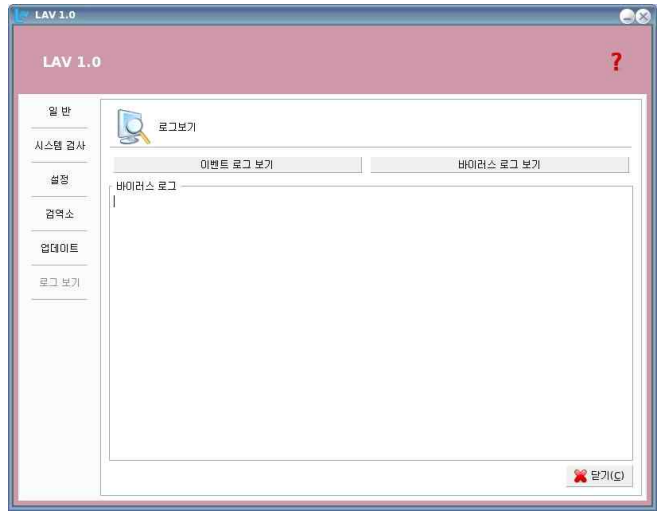
단계		항목/시험/결과
시험결과	2	1. 상기의 URL에서 다운로드한 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 일반 사용자로 변경하고, 파일 퍼미션은 666으로 수정한 후, 디렉토리는 777로 변경  2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인 

단계		항목/시험/결과
시험결과	2	3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인  4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인 

단계	항목/시험/결과	
시험결과	3	1. 상기의 URL에서 다운로드한 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 일반 사용자로 변경하고, 파일 퍼미션은 444로 수정한 후, 디렉토리는 777로 변경  2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인 

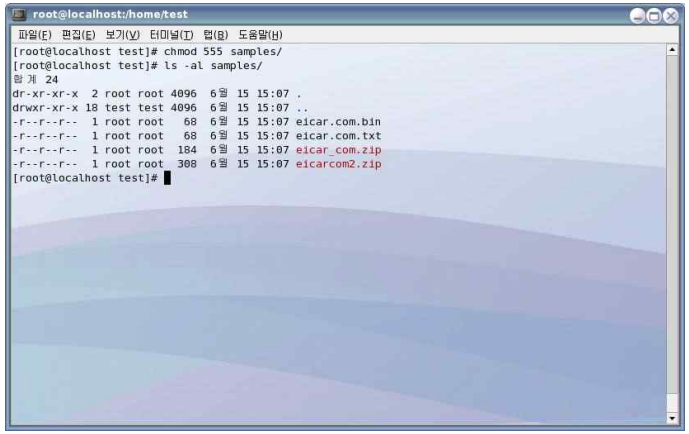
단계	항목/시험/결과	
시험결과	3	3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인  4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인 

단계	항목/시험/결과	
시험결과	4	1. 상기의 URL에서 다운로드한 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 root로 변경하고, 파일 퍼미션은 444로 수정한 후, 디렉토리는 777로 변경  2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인 

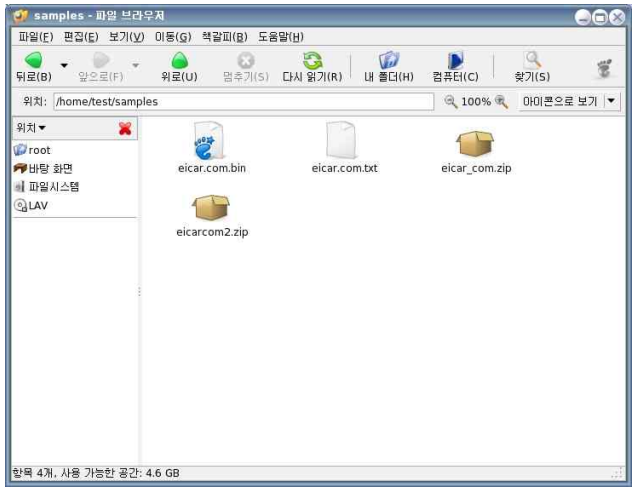
단계	항목/시험/결과	
시험결과	4	3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인  4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인 

단계	항목/시험/결과
시험결과	5

1. 상기의 URL에서 다운로드한 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 root로 변경하고, 파일 퍼미션은 444로 수정한 후, 디렉토리는 555로 변경

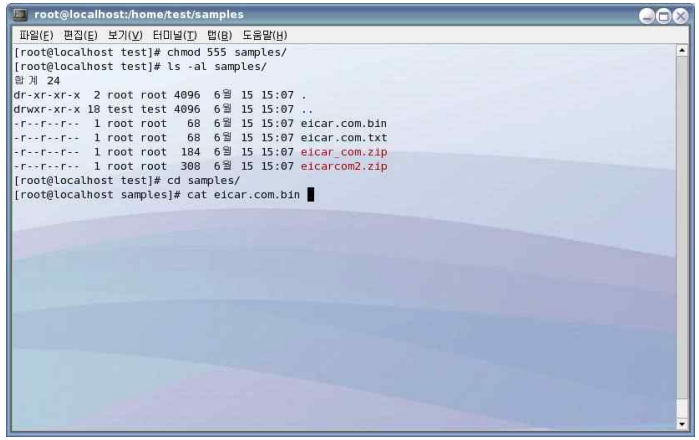


2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인

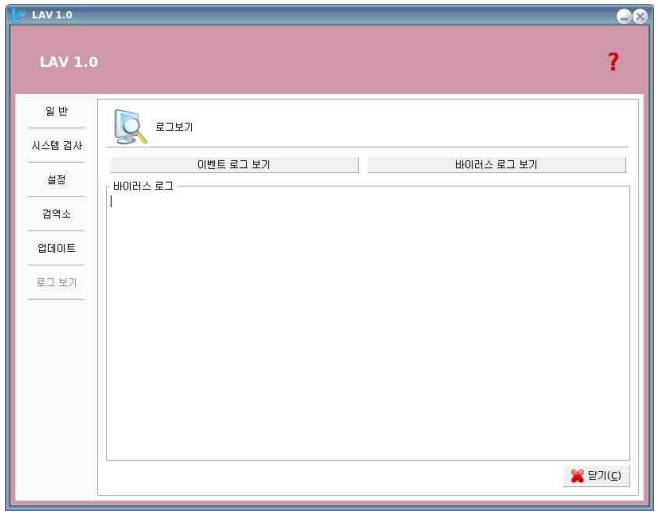


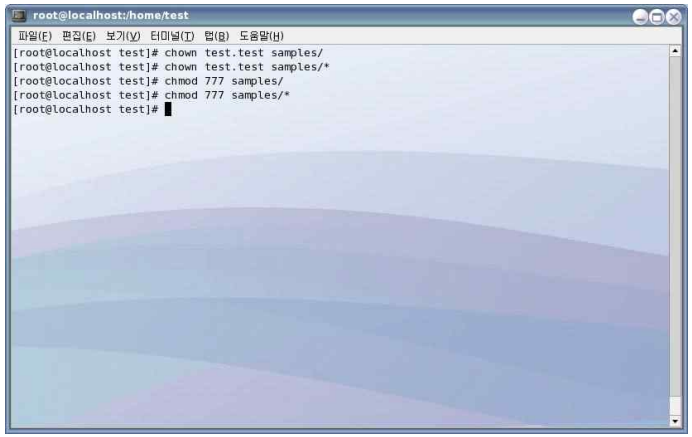
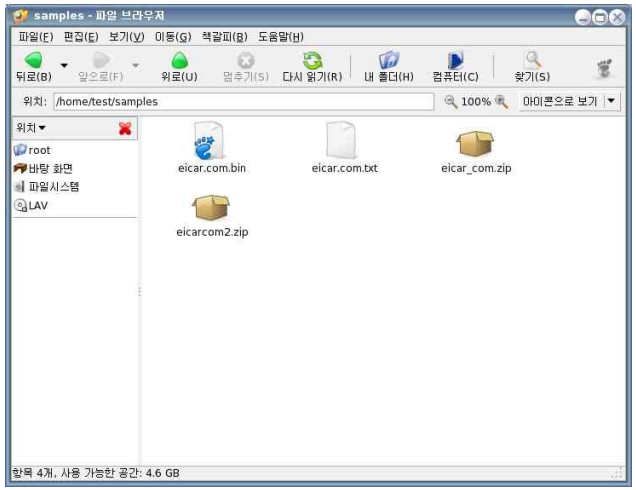
단계	항목/시험/결과
시험결과	5

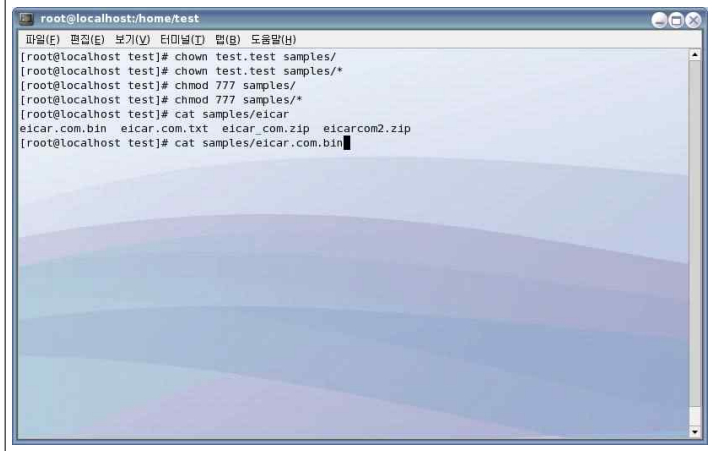
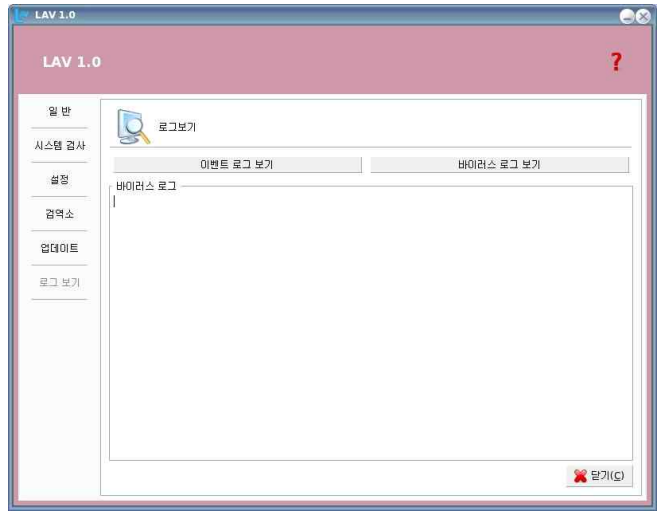
3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인

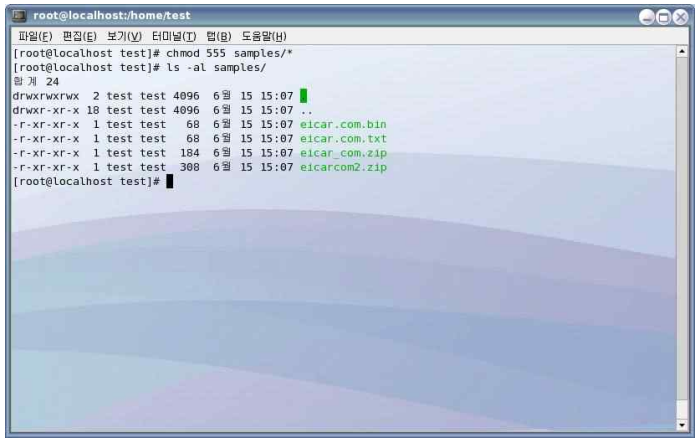
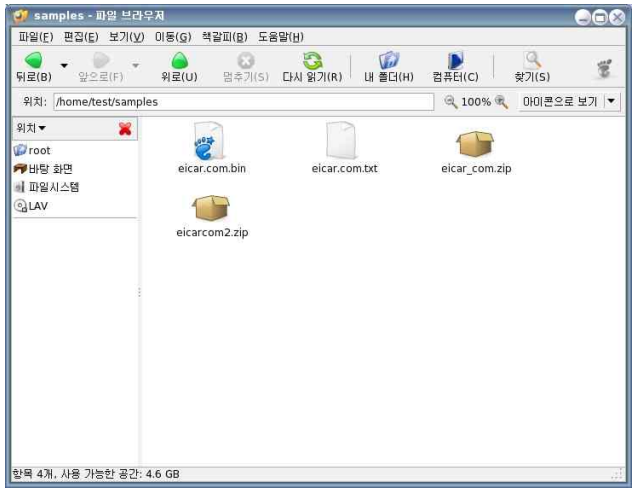


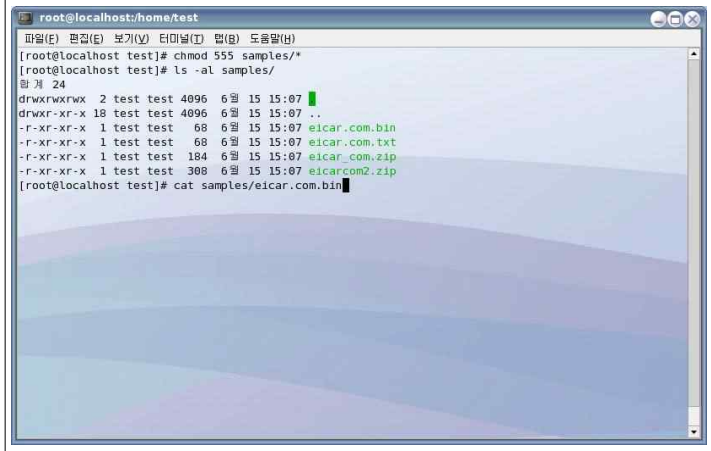
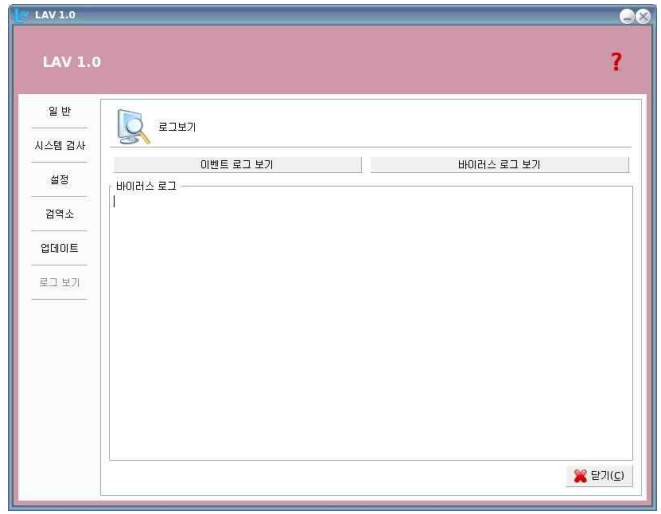
4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인

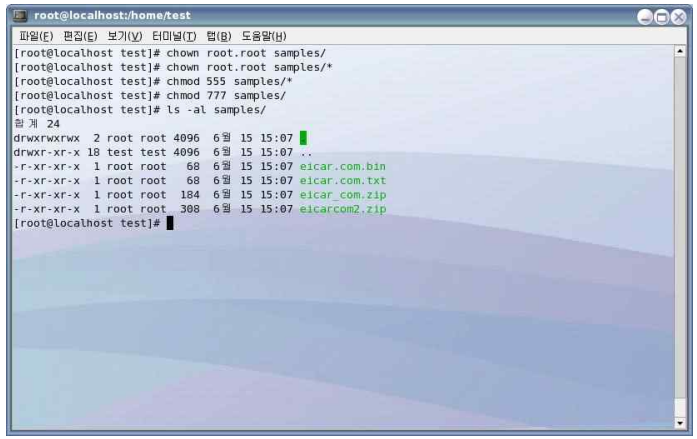
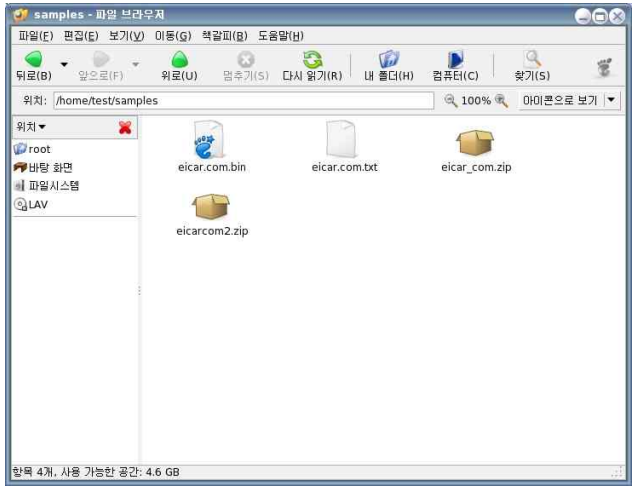


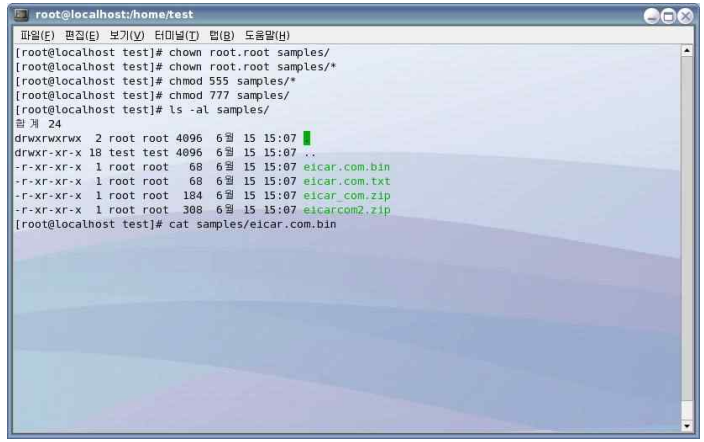
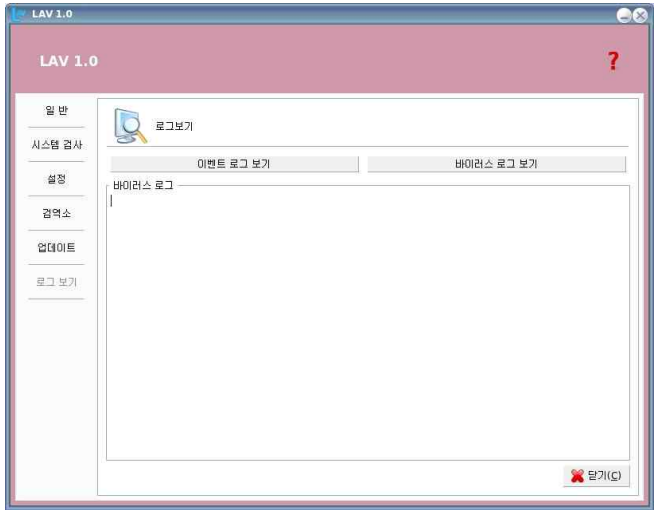
단계		항목/시험/결과
시험결과	6	1. 상기의 URL에서 다운로드한 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 일반 사용자로 변경하고, 파일과 디렉토리 퍼미션을 777로 수정  2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인 

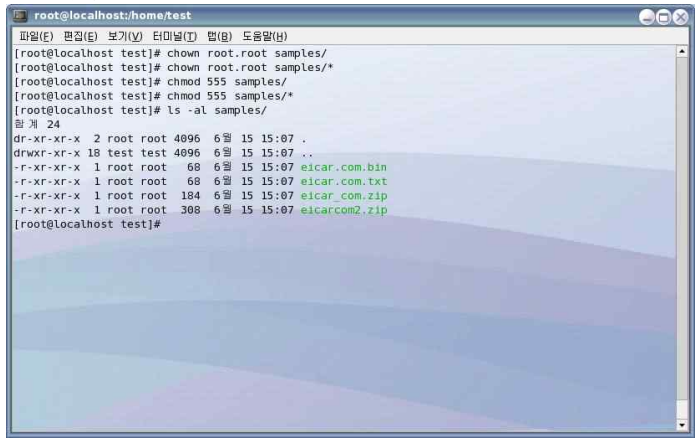
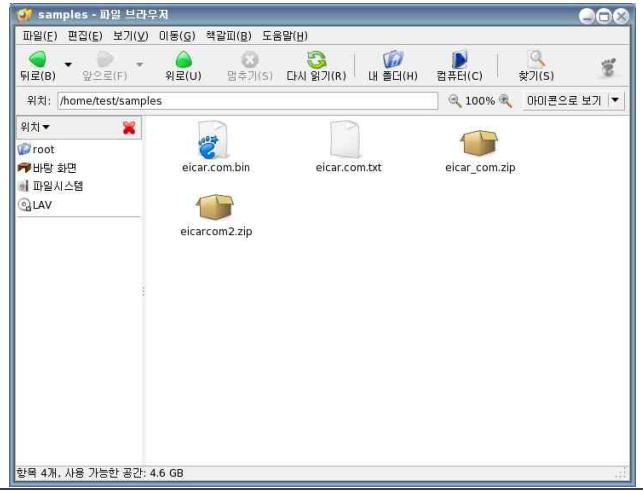
단계		항목/시험/결과
시험결과	6	3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인  4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인 

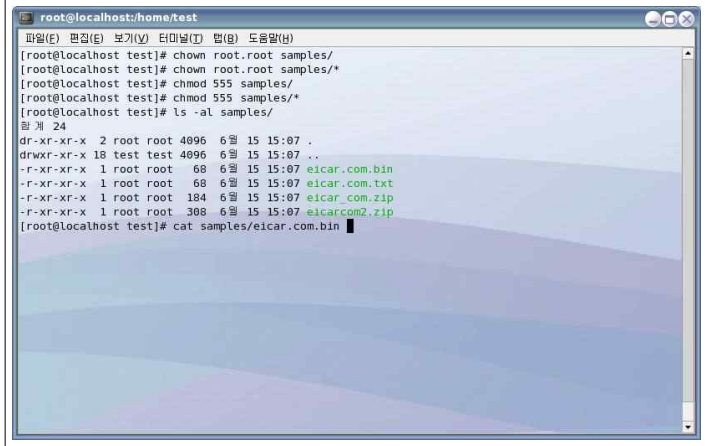
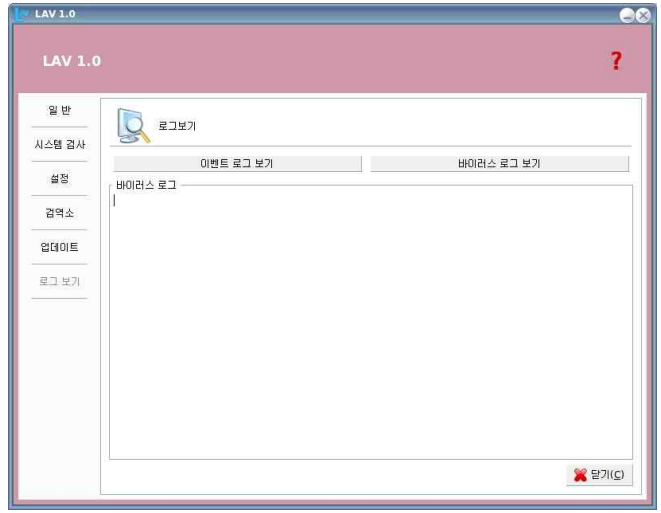
단계		항목/시험/결과
시험결과	7	1. 상기의 URL에서 다운로드한 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 일반 사용자로 변경하고, 파일 퍼미션은 555, 디렉토리 퍼미션은 777로 수정  2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인 

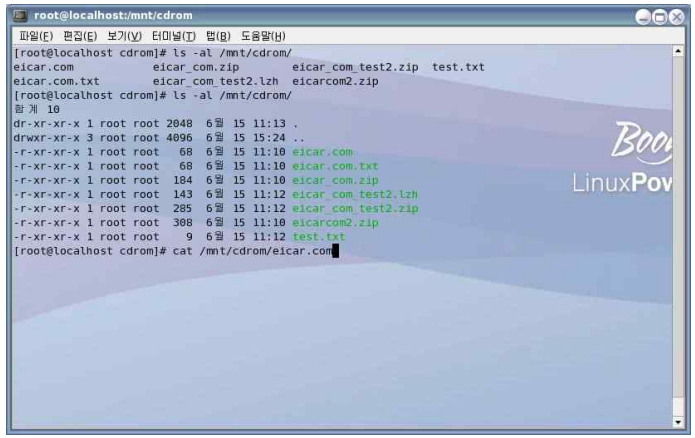
단계		항목/시험/결과
시험결과	7	3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인  4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인 

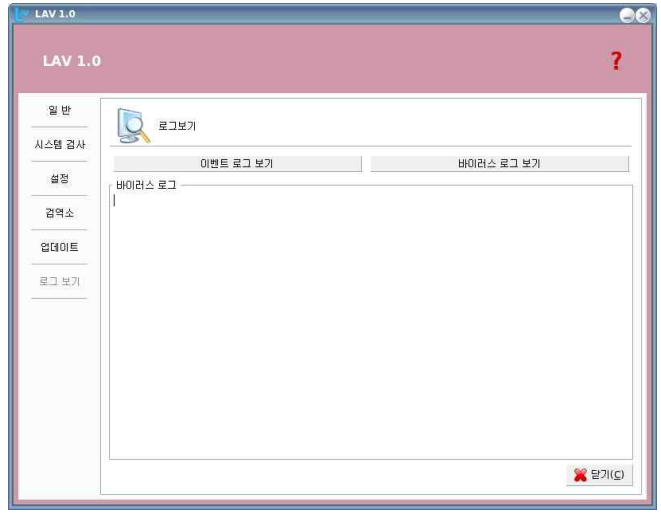
단계		항목/시험/결과
시험결과	8	1. 상기의 URL에서 다운로드한 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 root로 변경하고, 파일 퍼미션은 555, 디렉토리 퍼미션은 777로 수정  2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인 

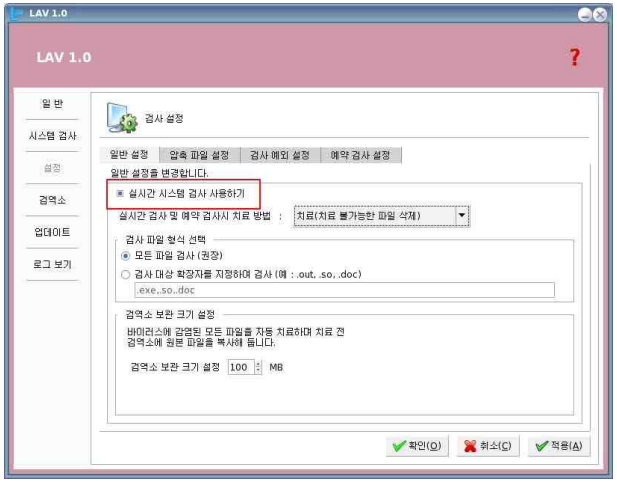
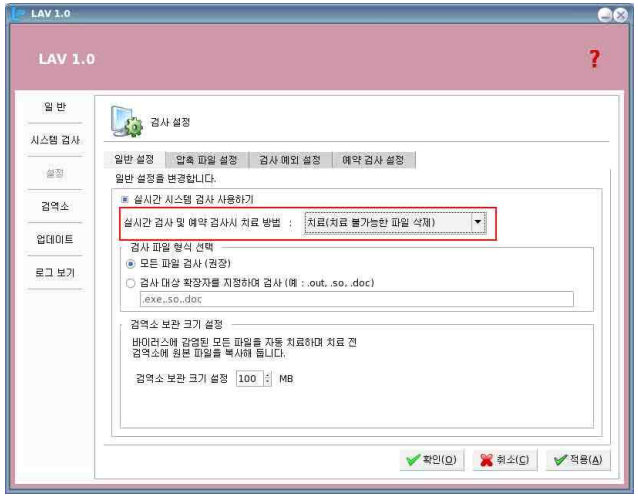
단계		항목/시험/결과
시험결과	8	3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인  4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인 

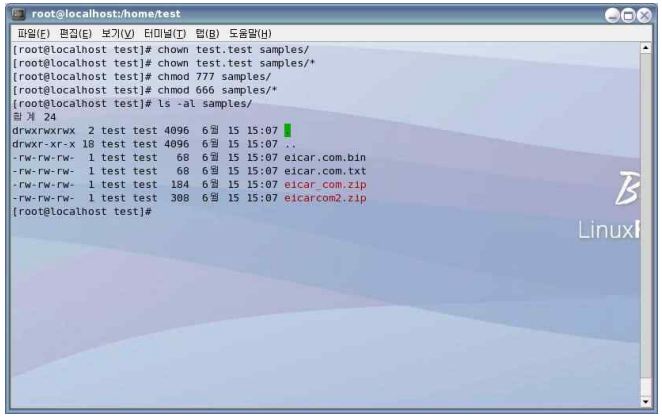
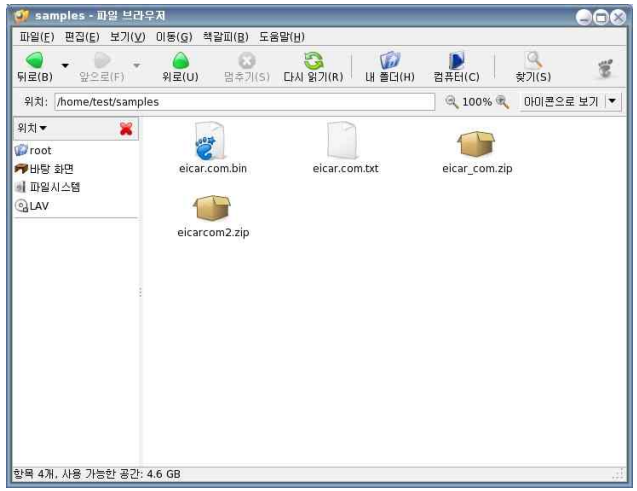
단계		항목/시험/결과
시험결과	9	1. 상기의 URL에서 다운로드한 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 root로 변경하고, 파일 퍼미션과 디렉토리 퍼미션을 555로 수정  2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인 

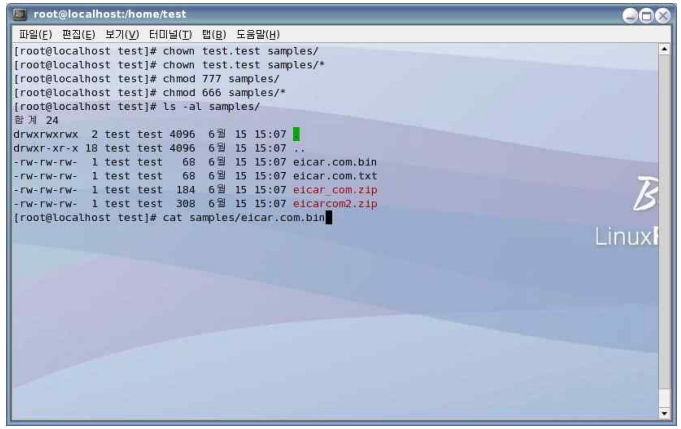
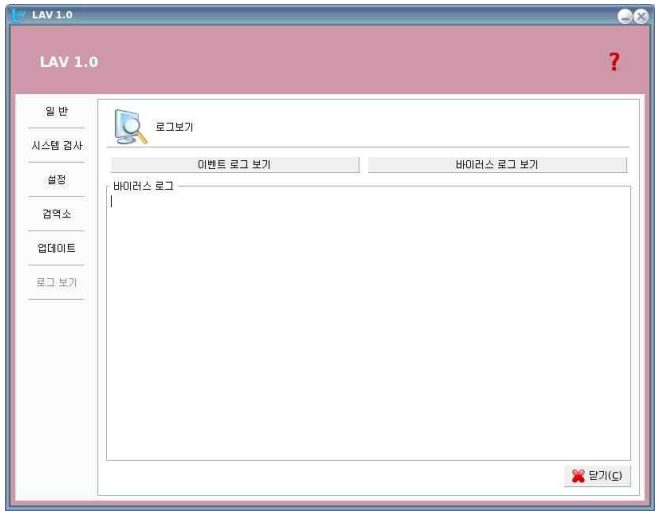
단계		항목/시험/결과
시험결과	9	3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인  4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인 

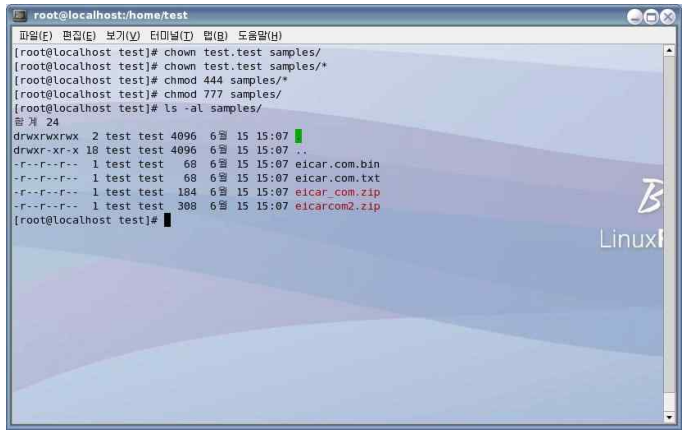
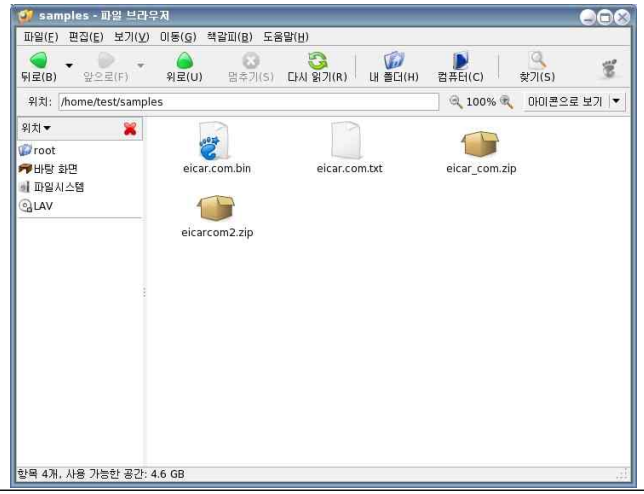
단계	항목/시험/결과	
시험결과	10	1. 바이러스 파일을 저장한 CD 매체를 삽입하고 CD 드라이브의 해당 파일을 열어, 접근이 가능한지 확인  2. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인 

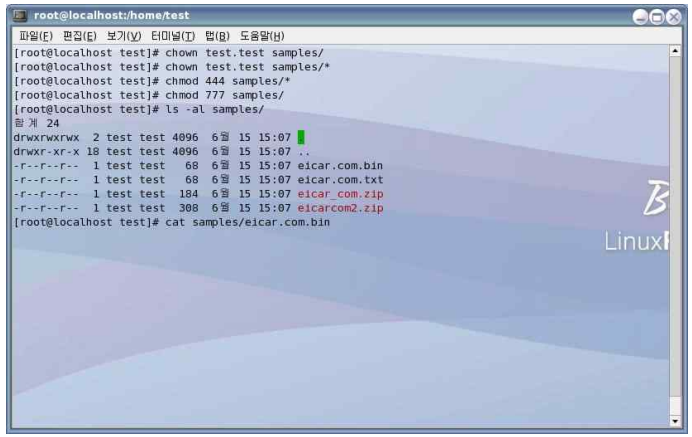
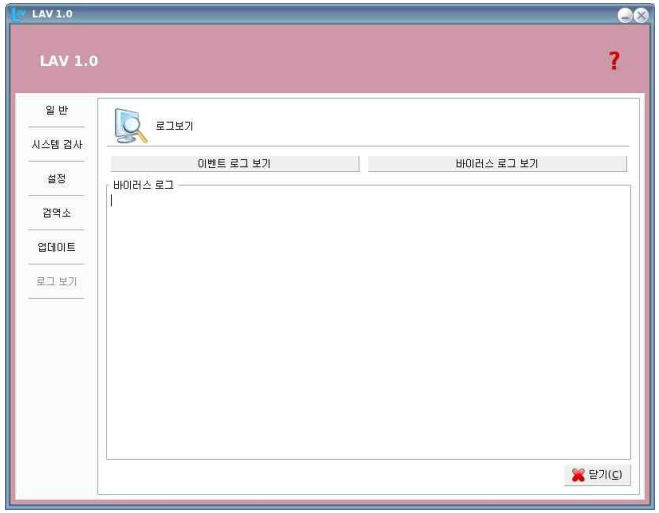
단계	항목/시험/결과	
시험결과	10	3. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인 

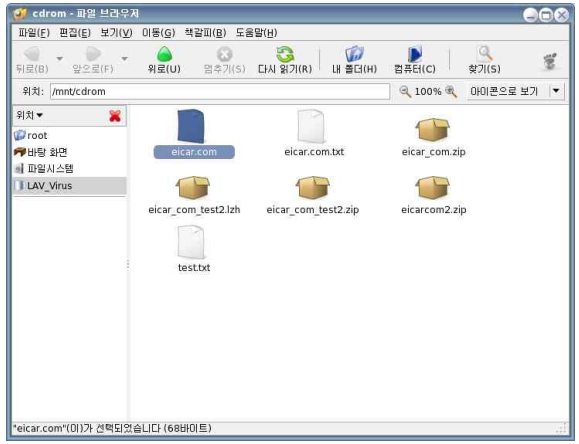
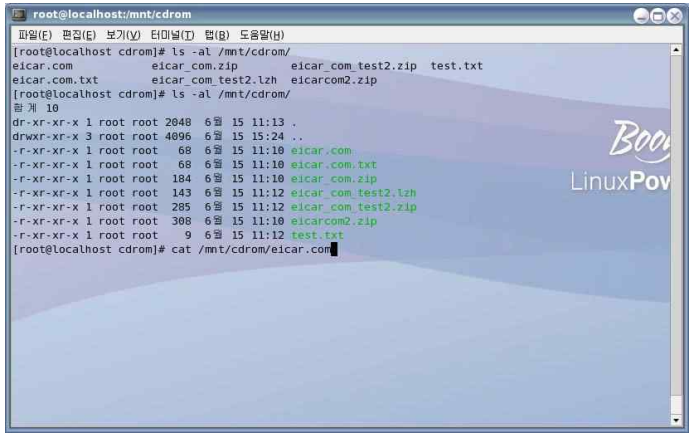
단계		항목/시험/결과
시험결과	11	1. [설정] 메뉴에서 '실시간 시스템 검사 사용하기'가 'On' 되어 있는지 확인하고, 만일 Off 이면 On 시킨다.  2. 실시간 검사 및 예약 검사시 치료 방법은 [치료(치료 불가능한 파일 삭제)]로 설정 

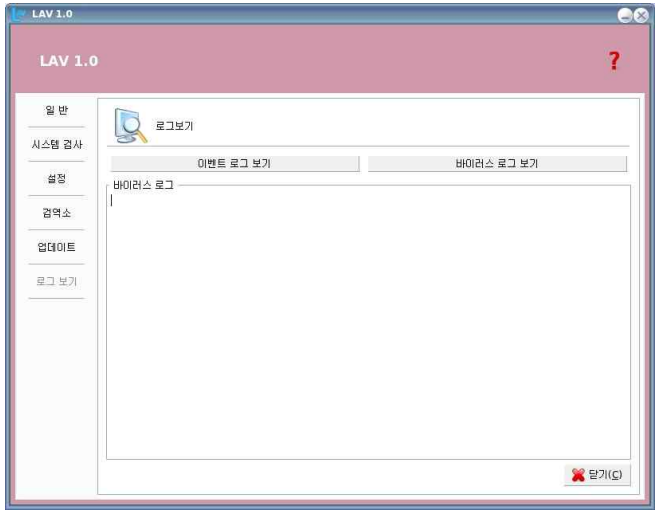
단계		항목/시험/결과
시험결과	12	1. 바이러스 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 일반 사용자로 변경하고, 파일 퍼미션은 666, 디렉토리 퍼미션은 777로 수정  2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인 

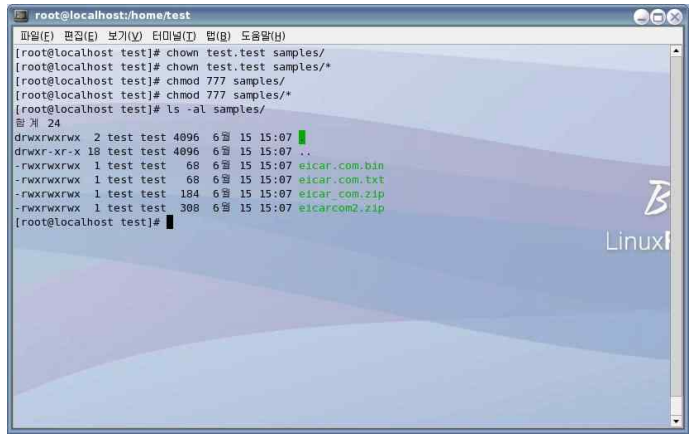
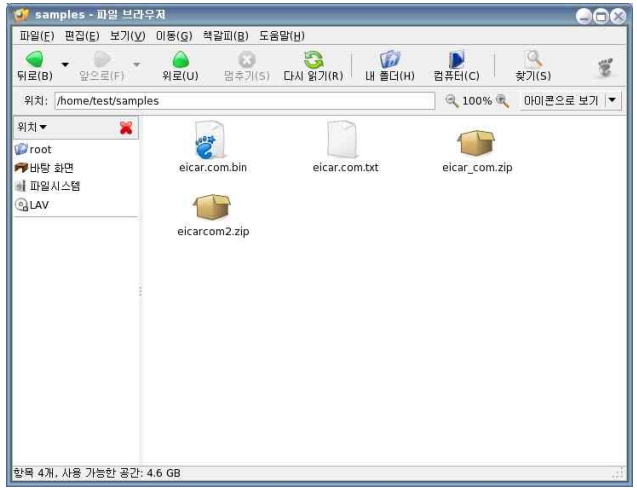
단계		항목/시험/결과
시험결과	12	3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인  4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인 

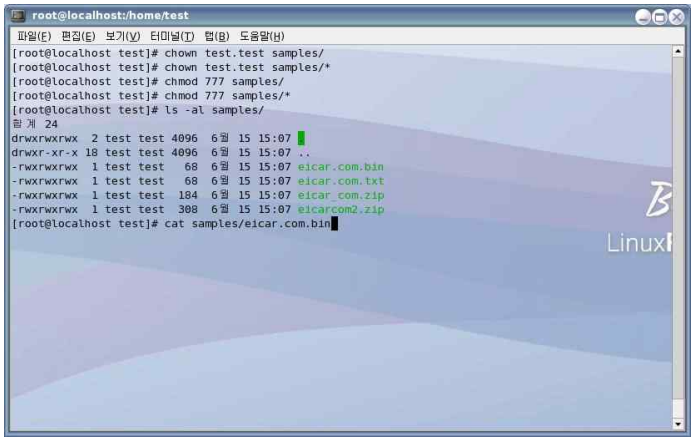
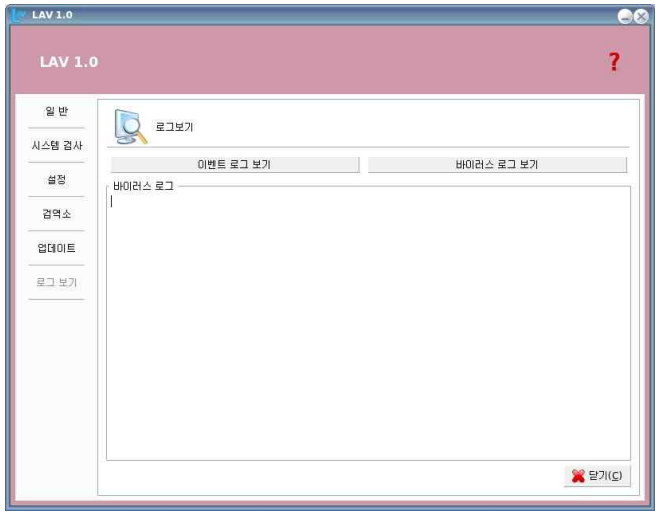
단계		항목/시험/결과
시험결과	13	1. 바이러스 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 일반 사용자로 변경하고, 파일 퍼미션은 444, 디렉토리 퍼미션은 777로 수정  2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인 

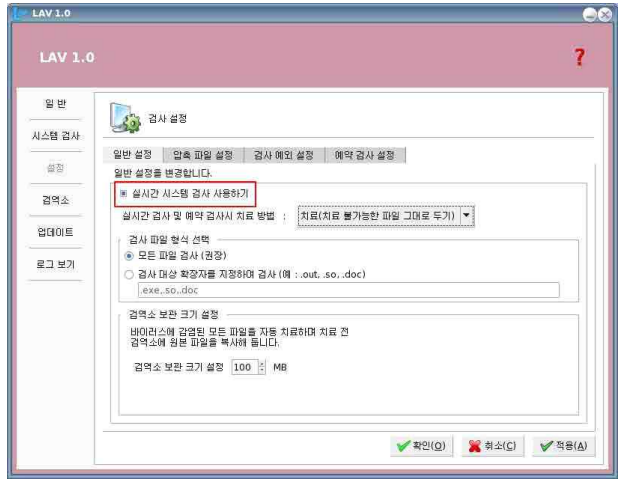
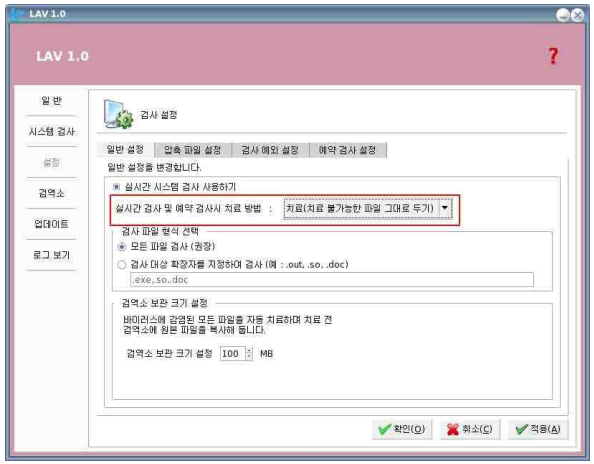
단계	항목/시험/결과	
시험결과	13	3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인  4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인 

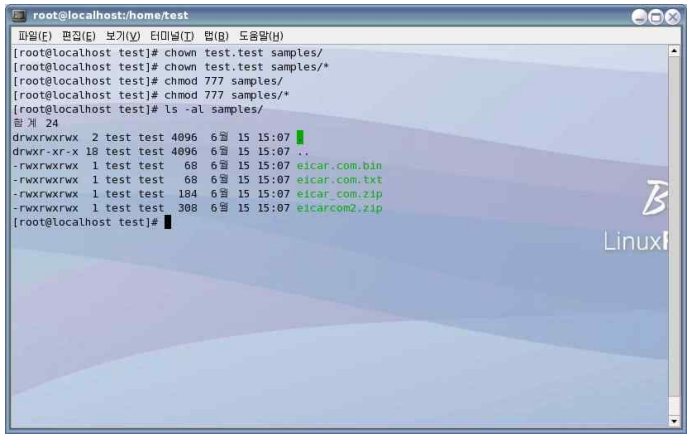
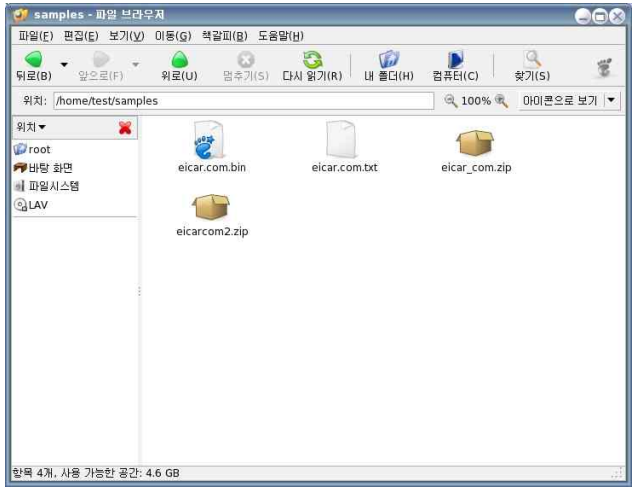
단계	항목/시험/결과	
시험결과	14	1. 바이러스 파일을 저장한 CD 매체를 삽입하고 CD 드라이브의 해당 파일을 열어, 접근이 가능한지 확인  2. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인 

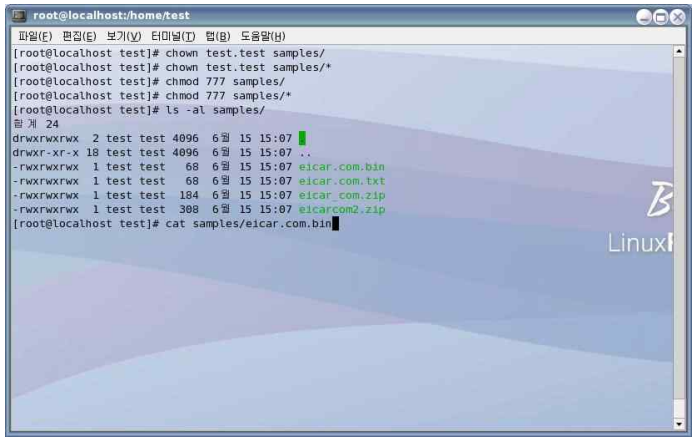
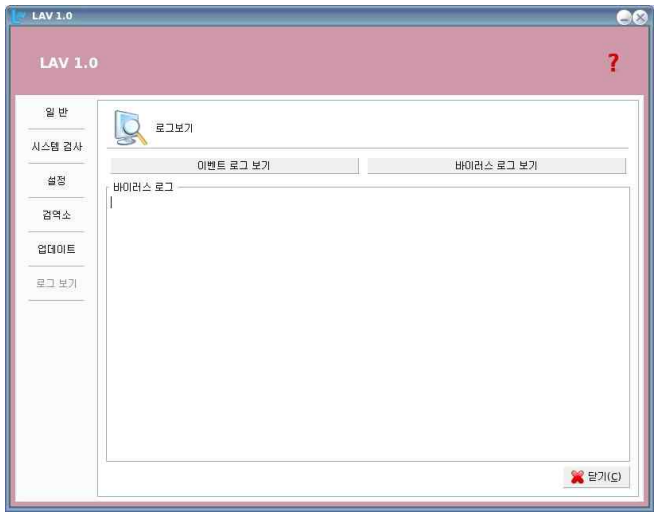
단계	항목/시험/결과	
시험결과	14	3. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인 

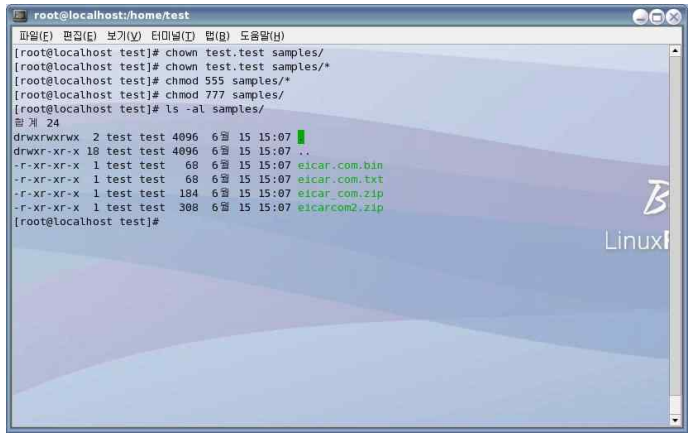
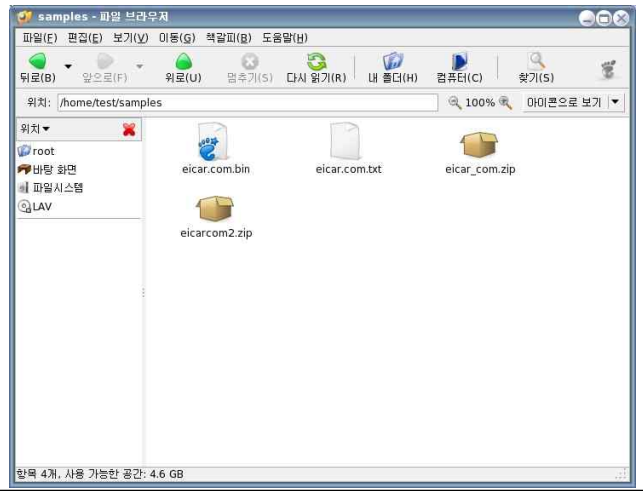
단계	항목/시험/결과	
시험결과	15	1. 바이러스 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 일반 사용자로 변경하고, 파일과 디렉토리 퍼미션을 777로 수정  2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인 

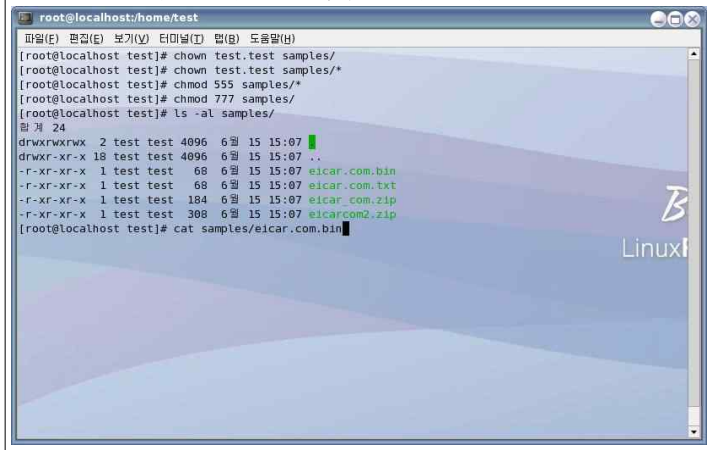
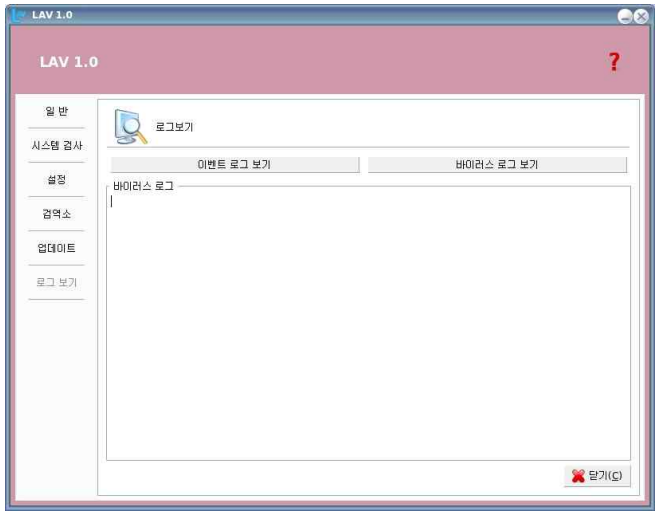
단계		항목/시험/결과
시험결과	15	3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인  4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인 

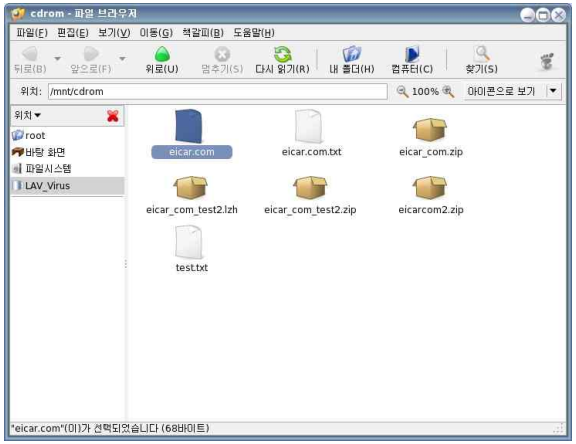
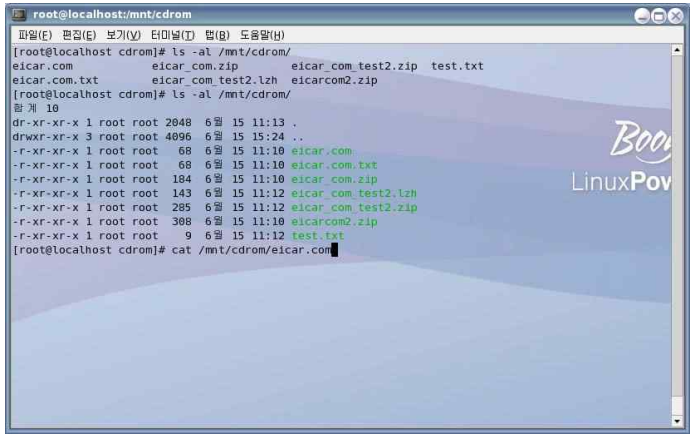
단계		항목/시험/결과
시험결과	16	1. [설정] 메뉴에서 '실시간 시스템 검사 사용하기' 가 'On' 되어 있는지 확인하고, 만일 Off 이면 On 시킨다.  2. 실시간 검사 및 예약 검사시 치료 방법은 [치료(치료 불가능한 파일 그대로 두기)]로 설정 

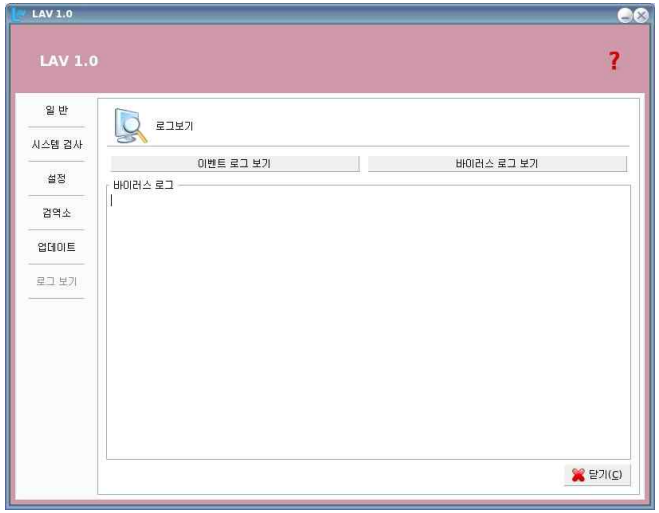
단계		항목/시험/결과
시험결과	17	1. 바이러스 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 일반 사용자로 변경하고, 파일과 디렉토리 퍼미션을 777로 수정  2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인 

단계		항목/시험/결과
시험결과	17	3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인  4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인 

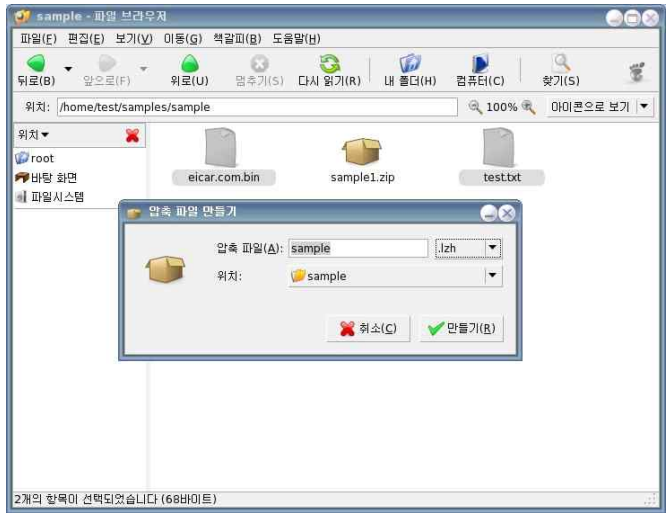
단계		항목/시험/결과
시험결과	18	1. 바이러스 파일을 저장한 디렉토리로 이동하여 해당 디렉토리와 파일의 소유권을 일반 사용자로 변경하고, 파일의 퍼미션을 555로, 디렉토리 퍼미션을 777로 수정  2. 저장된 디렉토리로 이동하여 해당 파일을 열어, 접근이 가능한지 확인 

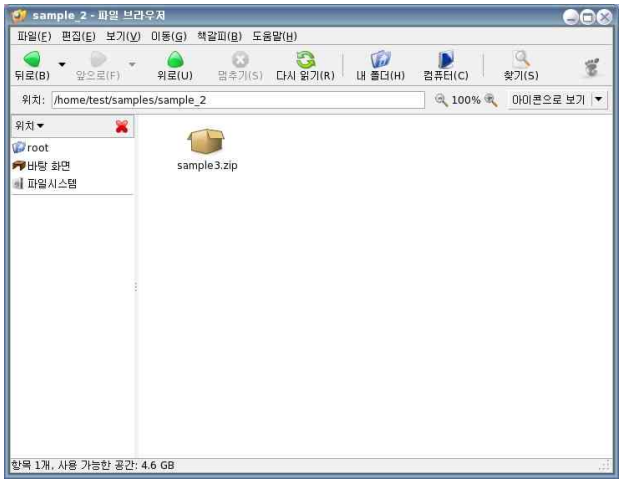
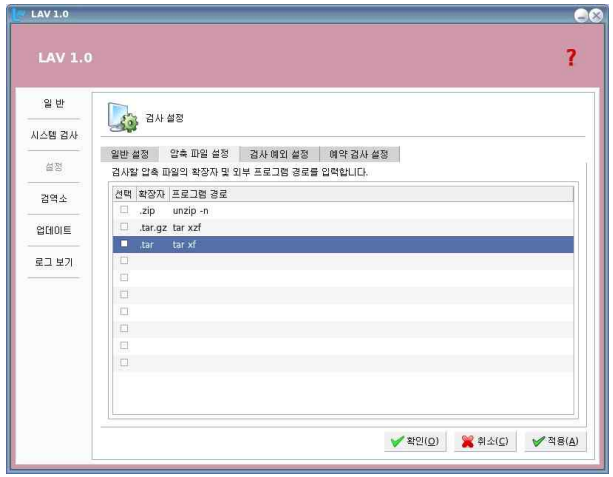
단계		항목/시험/결과
시험결과	18	3. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인  4. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인 

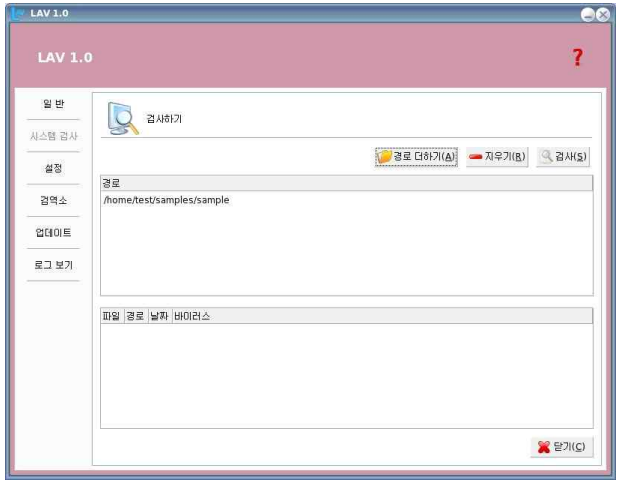
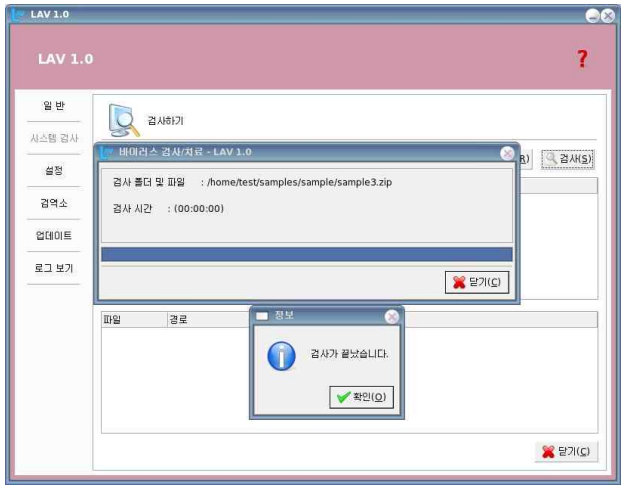
단계		항목/시험/결과
시험결과	19	1. 바이러스 파일을 저장한 CD 매체를 삽입하고 CD 드라이브의 해당 파일을 열어, 접근이 가능한지 확인  2. 쉘프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인 

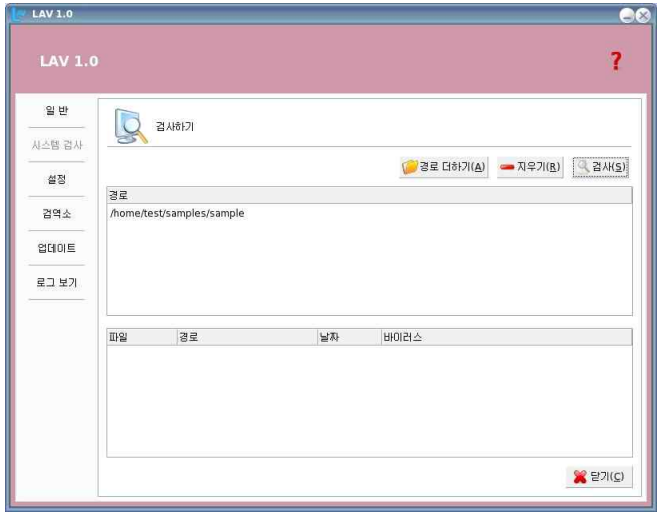
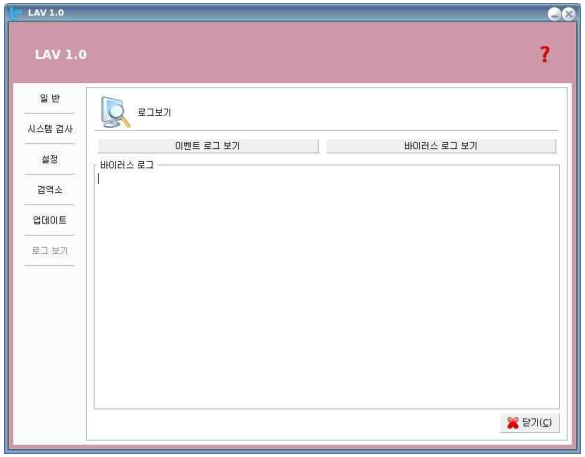
단계		항목/시험/결과
시험결과	19	3. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인 

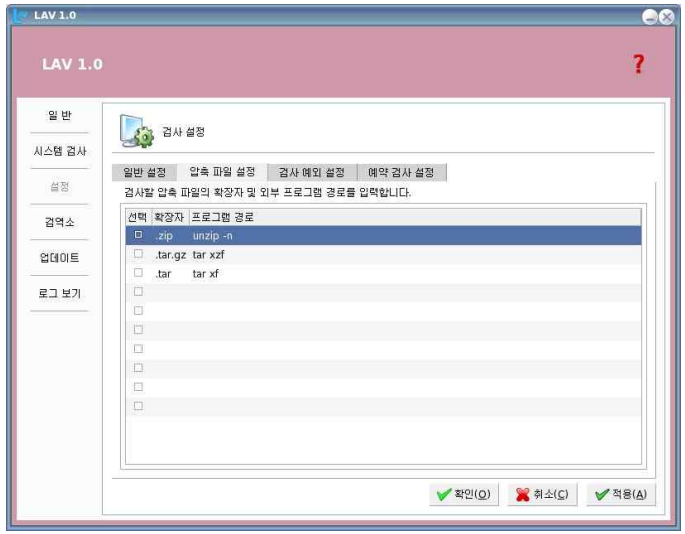
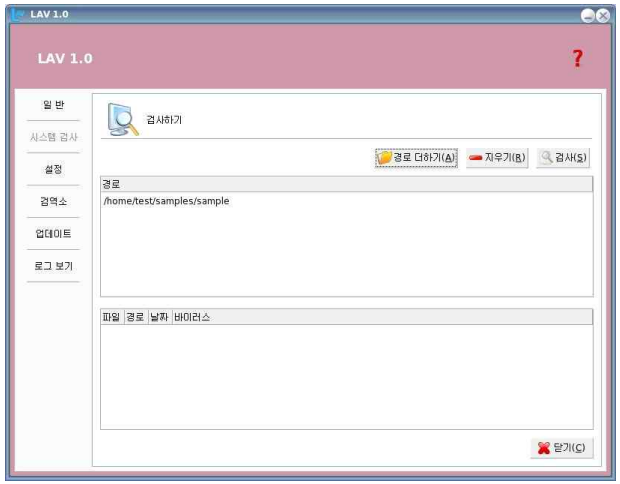
단계	항목/시험/결과	
시험절차	시험항목	LAV의 수동 검사
	1	1. X-windows로 로그인한 후, LAV를 실행시킨다. 2. 바이러스 파일과 일반 정상 파일을 zip 포맷으로 압축하고 저장한다. 3. 바이러스 파일과 일반 정상 파일을 lzh 포맷으로 압축하고 저장한다. 4. 바이러스 파일과 일반 정상 파일을 zip 포맷으로 이중 압축하고 상기의 파일이 저장된 디렉토리와 다른 디렉토리에 저장한다.
	2	1. [설정] > [압축 파일 설정] 메뉴에서 모든 압축파일 확장자의 체크박스를 해제한다. 2. [시스템 검사] 메뉴에서 해당 압축파일들이 저장된 디렉토리를 추가한다. 3. 검사를 실행한다. 4. 결과 화면을 확인한다. 5. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되지 않았는지 확인한다.
	3	1. [설정] > [압축 파일 설정] 메뉴에서 zip 확장자의 체크박스를 선택한다. 2. [시스템 검사] 메뉴에서 해당 압축파일이 저장된 디렉토리를 추가한다. 3. 검사를 실행한다. 4. 결과 화면을 확인한다. 5. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.
	4	1. [설정] > [압축 파일 설정] 메뉴에서 lzh 확장자를 추가하고 체크박스를 선택한다. 2. [시스템 검사] 메뉴에서 해당 압축파일이 저장된 디렉토리를 추가한다. 3. 검사를 실행한다. 4. 결과 화면을 확인한다. 5. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.
	5	1. [설정] > [압축 파일 설정] 메뉴에서 zip 확장자의 체크박스를 선택한다. 2. [시스템 검사] 메뉴에서 이중 압축파일이 저장된 디렉토리를 추가한다. 3. 검사를 실행한다. 4. 결과 화면을 확인한다. 5. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.
시험결과	1	1. X-windows로 로그인한 후, LAV 실행 2. 바이러스 파일과 일반 정상 파일을 zip 포맷으로 압축하고 저장

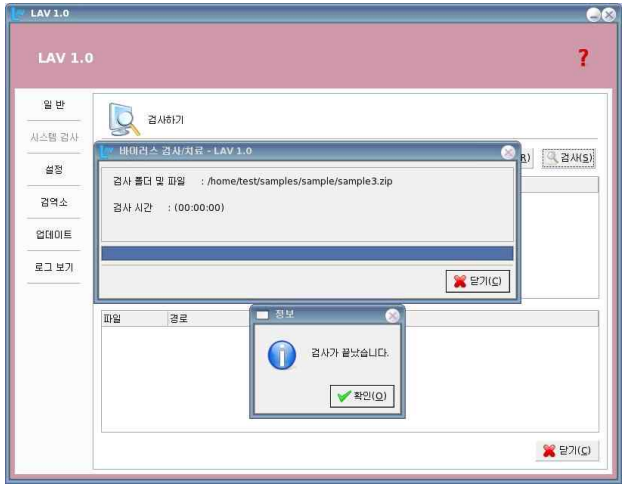
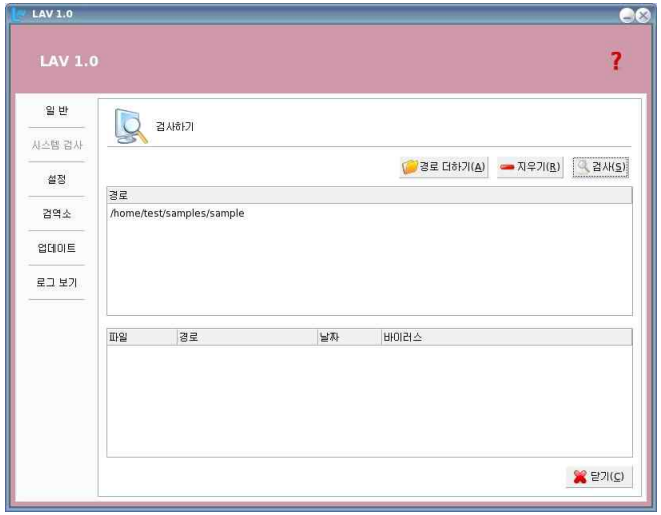
단계	항목/시험/결과	
시험결과	1	 3. 바이러스 파일과 일반 정상 파일을 lzh 포맷으로 압축하고 저장 

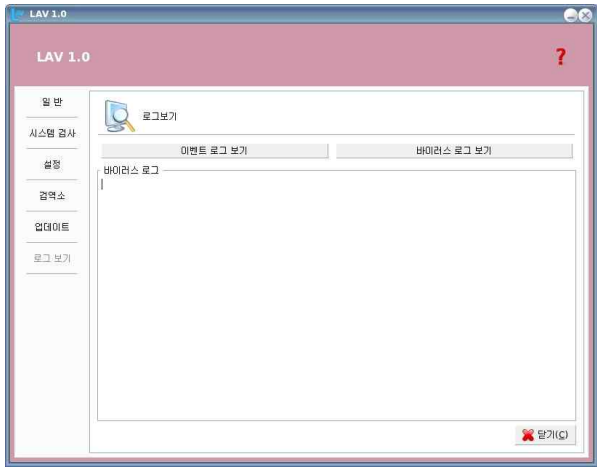
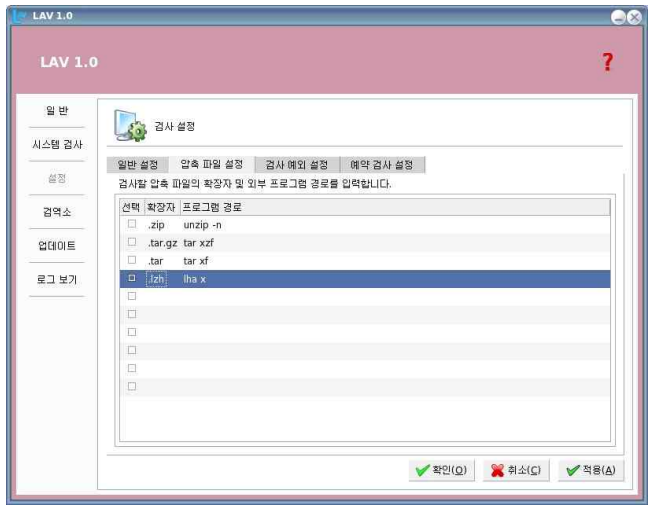
단계	항목/시험/결과	
시험결과	1	4. 바이러스 파일과 일반 정상 파일을 zip 포맷으로 이중 압축하고 상기의 파일이 저장된 디렉토리와 다른 디렉토리에 저장 
	2	1. [설정] > [압축 파일 설정] 메뉴에서 모든 압축파일 확장자의 체크박스 해제 

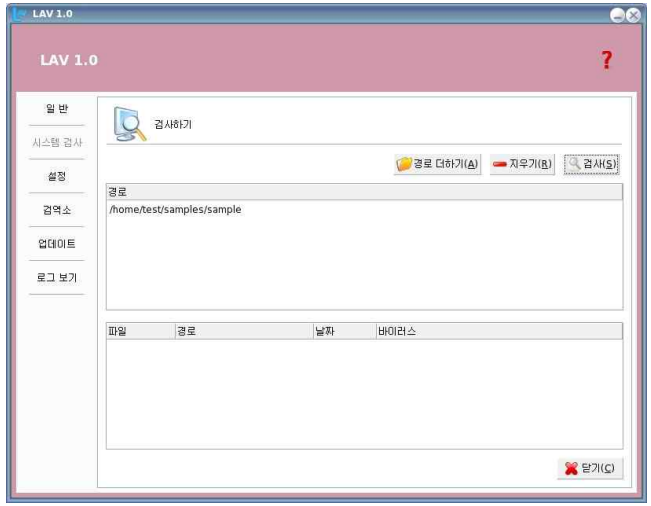
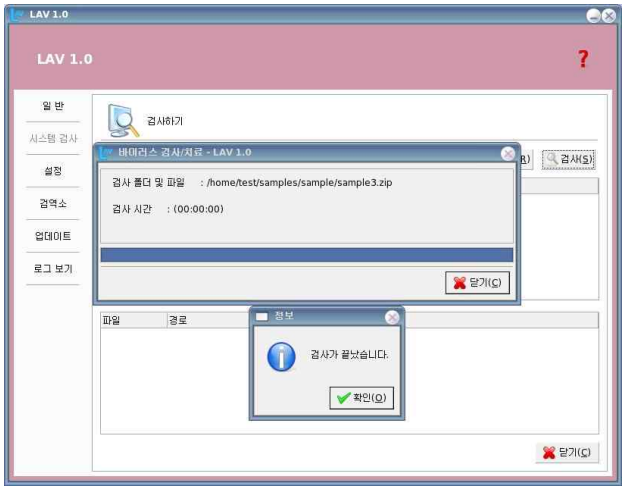
단계	항목/시험/결과	
시험결과	2	2. [시스템 검사] 메뉴에서 해당 압축파일들이 저장된 디렉토리 추가  3. 검사 실행 

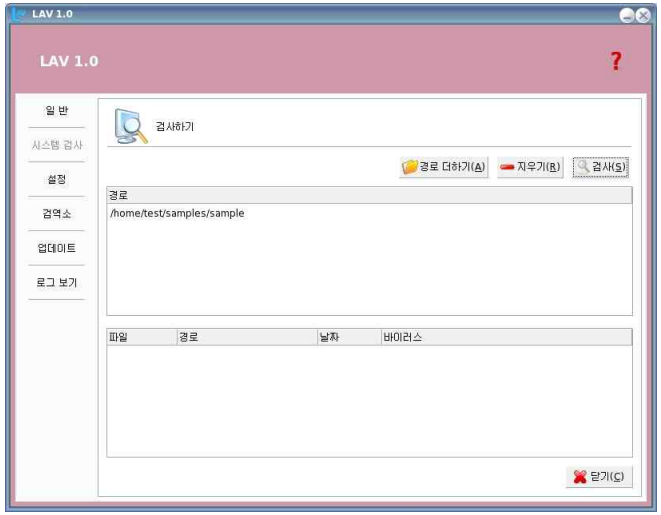
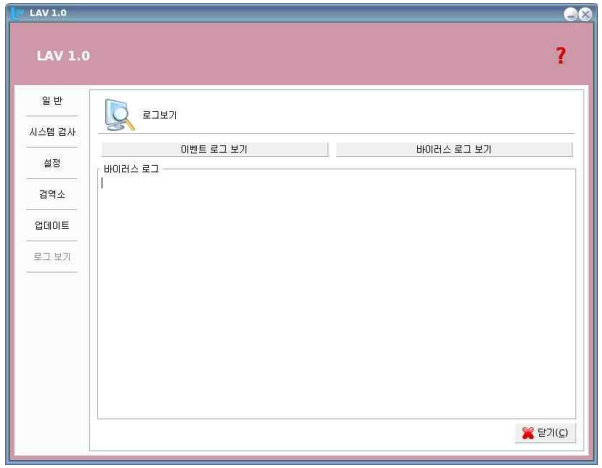
단계	항목/시험/결과	
시험결과	2	4. 결과 화면 확인  5. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인 

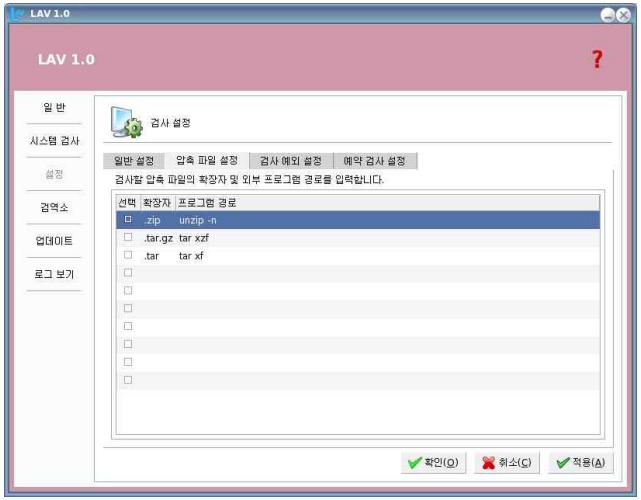
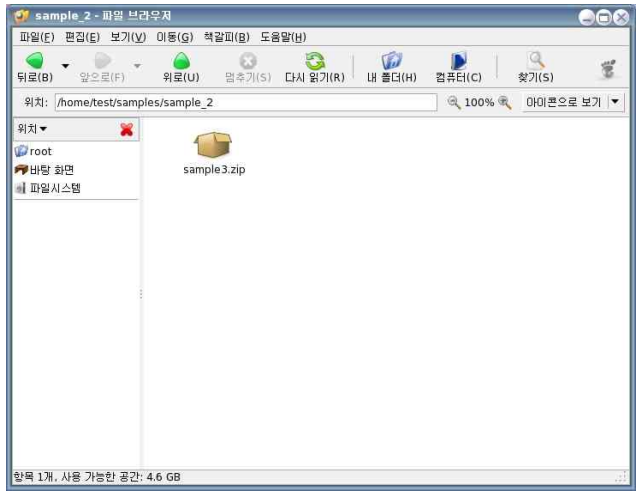
단계	항목/시험/결과	
시험결과	3	1. [설정] > [압축 파일 설정] 메뉴에서 zip 확장자의 체크박스 선택  2. [시스템 검사] 메뉴에서 해당 압축파일이 저장된 디렉토리 추가 

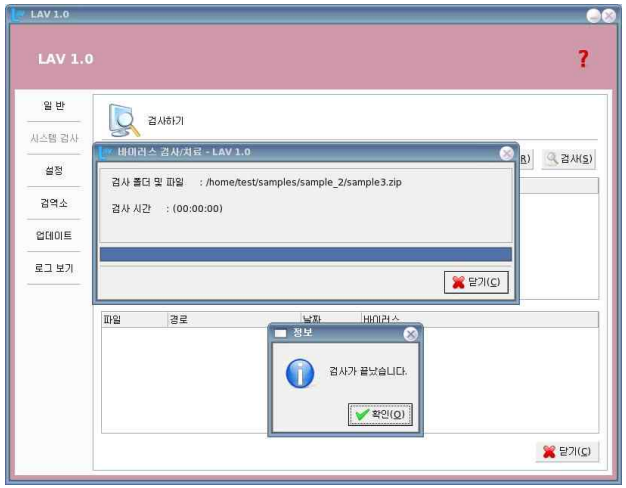
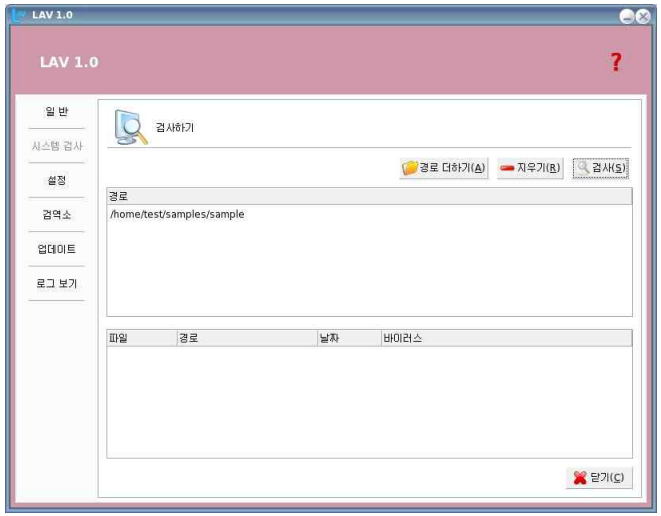
단계	항목/시험/결과	
시험결과	3	3. 검사 실행 
		4. 결과 화면 확인 

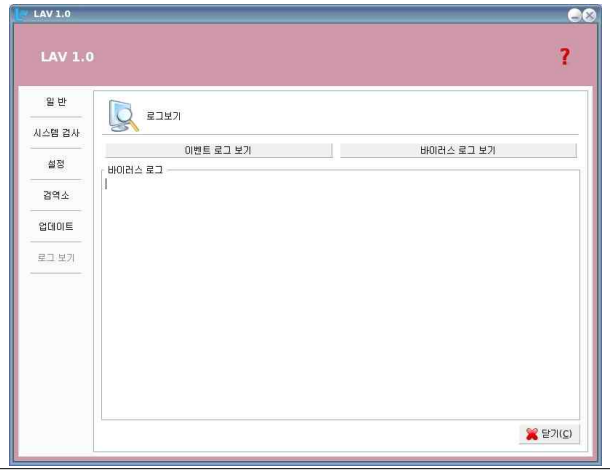
단계	항목/시험/결과	
시험결과	3	5. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인 
	4	1. [설정] > [압축 파일 설정] 메뉴에서 lzh 확장자를 추가하고 체크박스를 선 

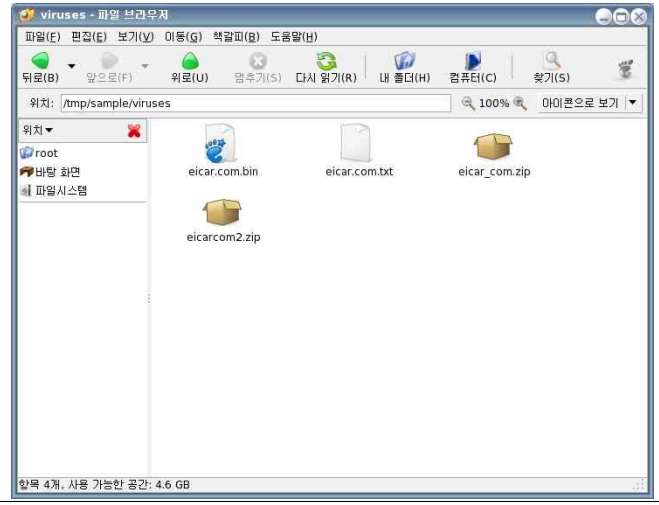
단계	항목/시험/결과	
시험결과	4	2. [시스템 검사] 메뉴에서 해당 압축파일이 저장된 디렉토리 추가  3. 검사 실행 

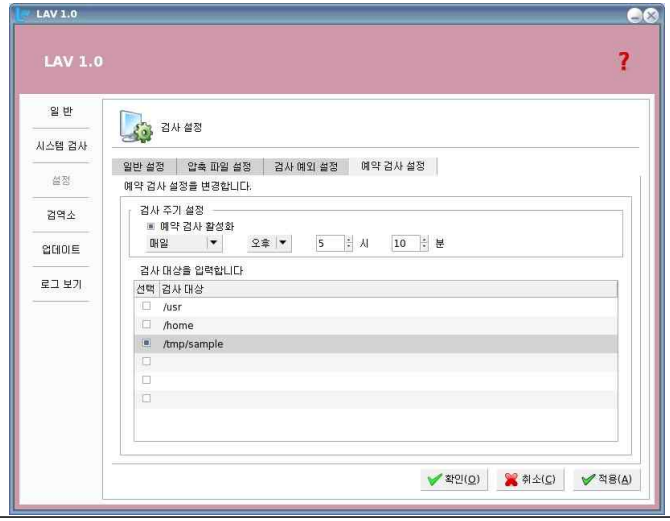
단계	항목/시험/결과	
시험결과	4	4. 결과화면 확인  5. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인 

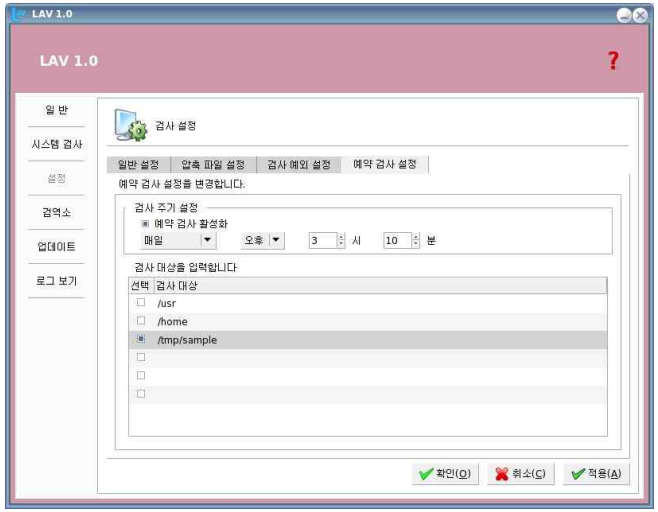
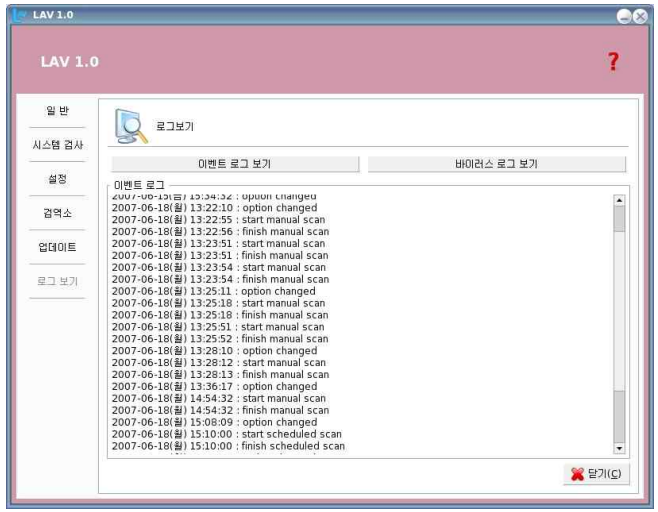
단계	항목/시험/결과
시험결과 5	1. [설정] > [압축 파일 설정] 메뉴에서 zip 확장자의 체크박스 선택  2. [시스템 검사] 메뉴에서 이중 압축파일이 저장된 디렉토리 추가 

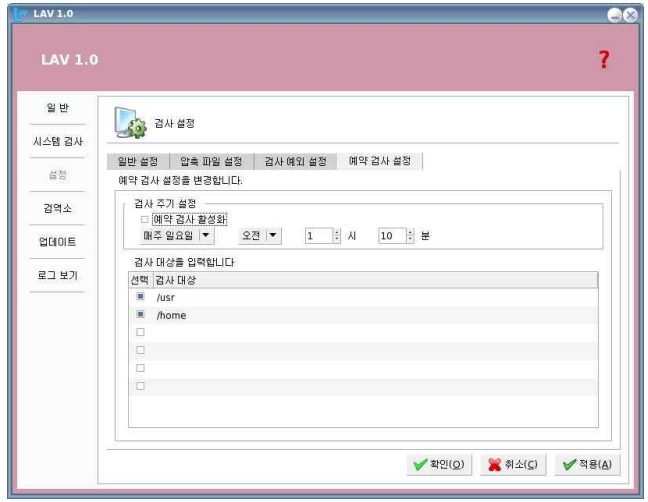
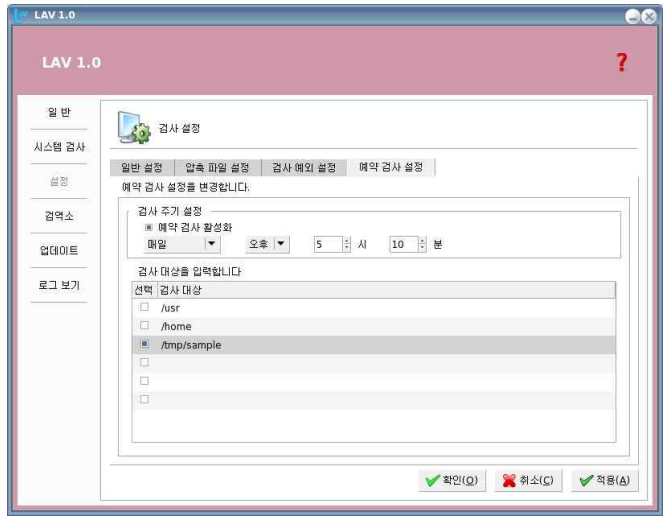
단계	항목/시험/결과
시험결과 5	3. 검사 실행  4. 결과 화면 확인 

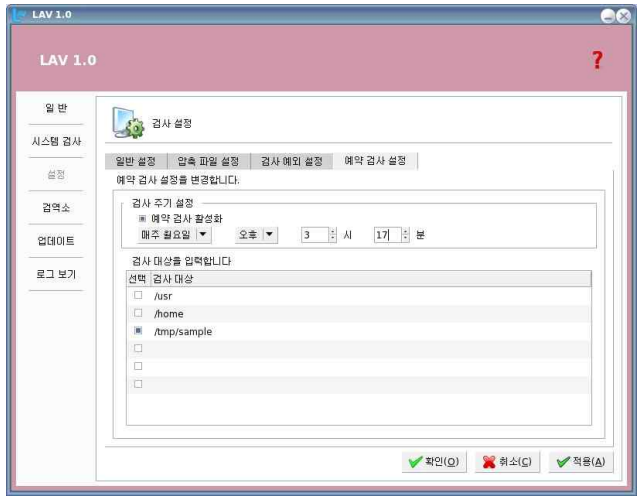
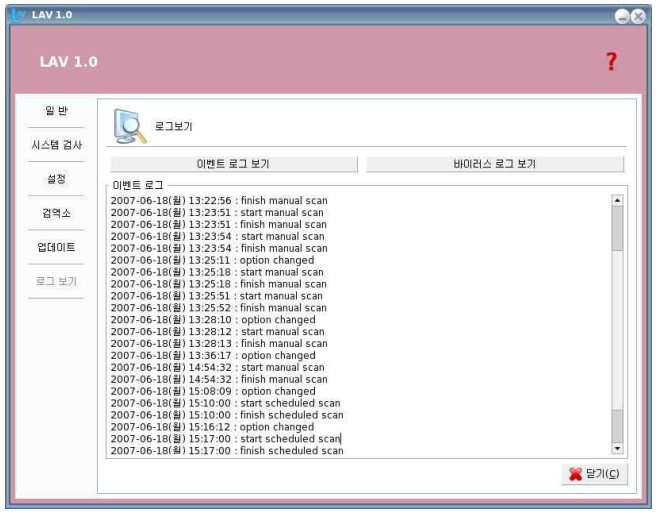
단계	항목/시험/결과	
시험결과	5	5. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인 
비 고		

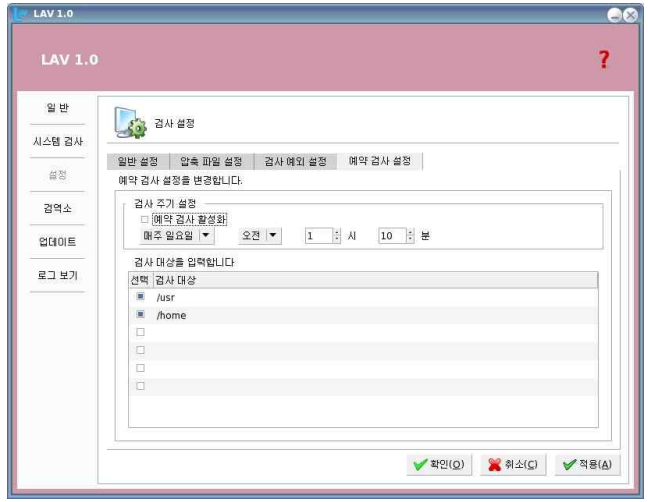
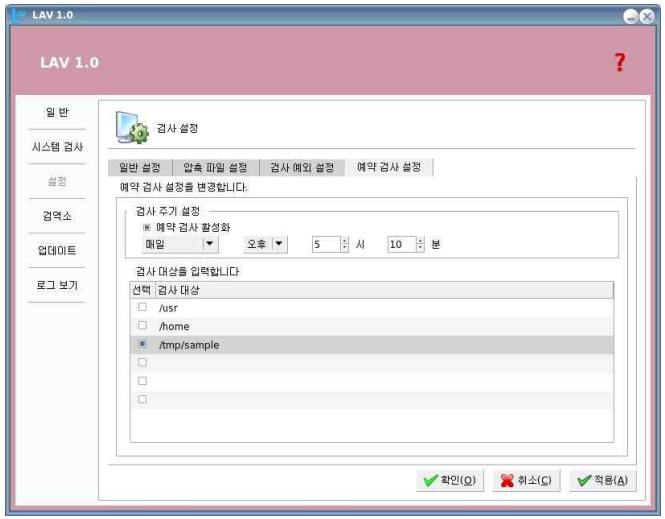
단계	항목/시험/결과	
시험절차	시험항목	예약 검사
	1	1. X-windows로 로그인하고 LAV를 실행시킨다. 2. 바이러스 파일을 저장한 디렉토리를 /tmp/sample 에 저장한다.
	2	1. [설정] 메뉴에서 '예약 검사 설정' 메뉴를 선택한다. 2. 검사 대상 리스트에서 빈 라인을 더블클릭하고, /tmp/sample 을 추가 설정한다. 3. 검사 주기를 '매일', 시간도 설정하고 '확인'을 누른다. 4. 해당 시간에 예약 검사 기능으로 제대로 검사가 수행되는지 확인한다.
	3	1. [설정] 메뉴에서 '예약 검사 설정' 메뉴를 선택한다. 2. 검사 대상 리스트에서 빈 라인을 더블클릭하고, /tmp/sample 을 추가 설정한다. 3. 검사 주기를 '특정 요일', 시간도 설정하고 '확인'을 누른다. 4. 해당 요일의 시간에 예약 검사 기능으로 제대로 검사가 수행되는지 확인한다.
	4	1. [설정] 메뉴에서 '예약 검사 설정' 메뉴를 선택한다. 2. 검사 대상 리스트에서 빈 라인을 더블클릭하고, /tmp/sample 을 추가 설정한다. 3. 검사 주기를 '특정 요일', 시간도 설정하고 '확인'을 누른다. 4. 해당 요일이 아닌 날의 시간에 예약 검사 기능이 수행되지는 않는지 확인한다.
시험결과	1	1. X-windows로 로그인하고 LAV 실행 2. 바이러스 파일을 저장한 디렉토리를 /tmp/sample 에 저장 

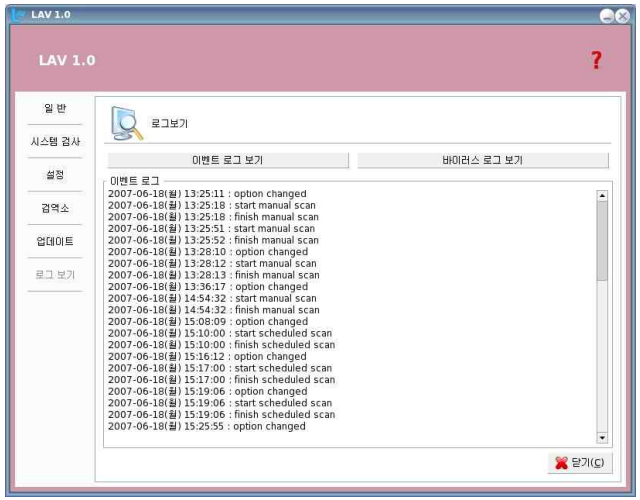
단계	항목/시험/결과	
시험결과	2	1. [설정] 메뉴에서 '예약 검사 설정' 메뉴 선택  2. 검사 대상 리스트에서 빈 라인을 더블클릭하고, /tmp/sample 을 추가 설정 

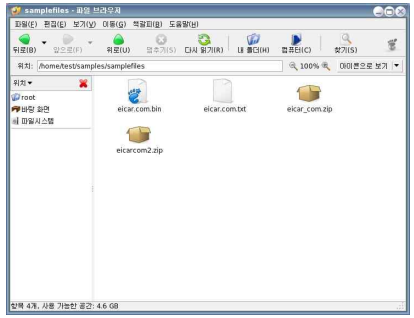
단계	항목/시험/결과	
시험결과	2	3. 검사 주기를 '매일', 시간도 설정하고 '확인'  4. 해당 시간에 예약 검사 기능으로 제대로 검사가 수행되는지 확인 

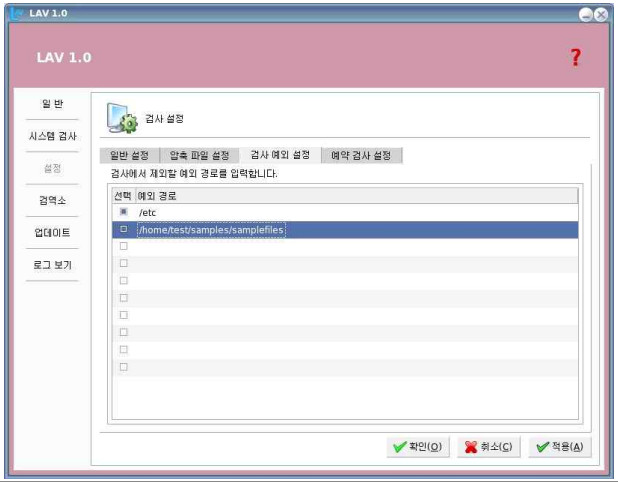
단계	항목/시험/결과	
시험결과	3	1. [설정] 메뉴에서 '예약 검사 설정' 메뉴 선택  2. 검사 대상 리스트에서 빈 라인을 더블클릭하고, /tmp/sample 을 추가 설정 

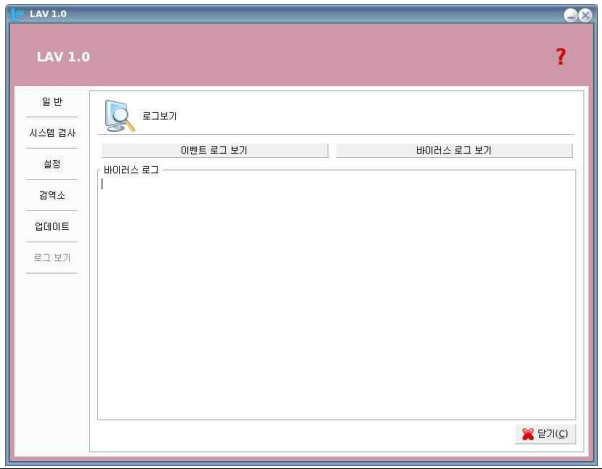
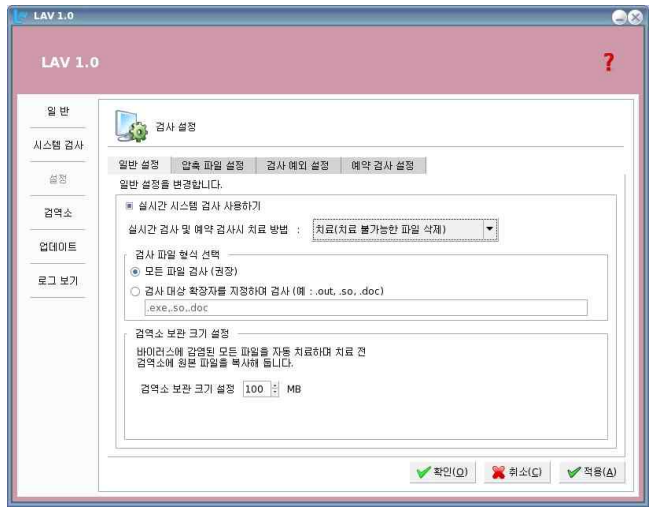
단계		항목/시험/결과
시험결과	3	3. 검사 주기를 '특정 요일', 시간도 설정하고, '확인'  4. 해당 요일의 시간에 예약 검사 기능으로 제대로 검사가 수행되는지 확인 

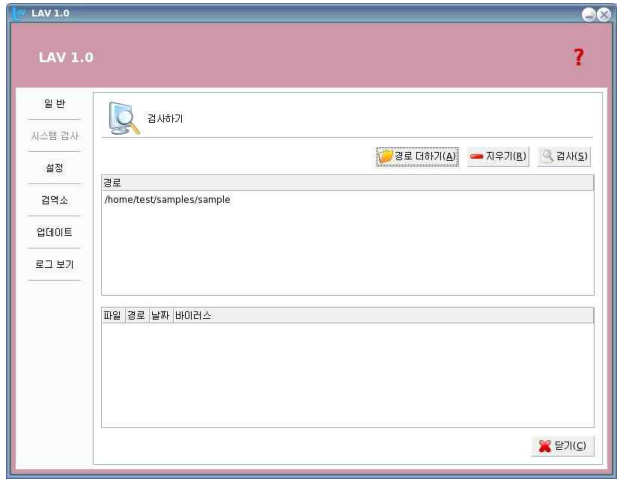
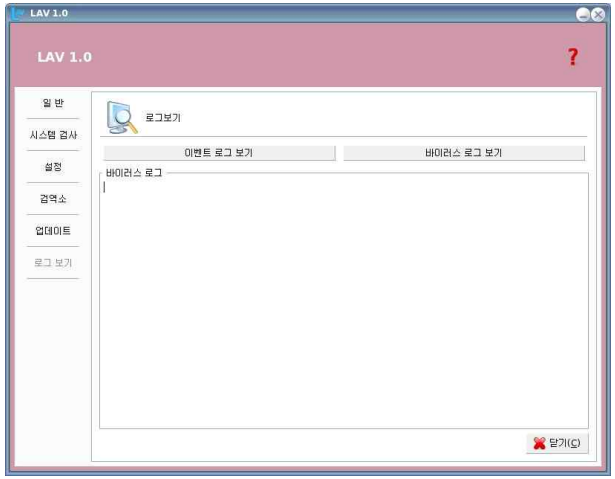
단계		항목/시험/결과
시험결과	4	1. [설정] 메뉴에서 '예약 검사 설정' 메뉴 선택  2. 검사 대상 리스트에서 빈 라인을 더블클릭하고, /tmp/sample 을 추가 설정 

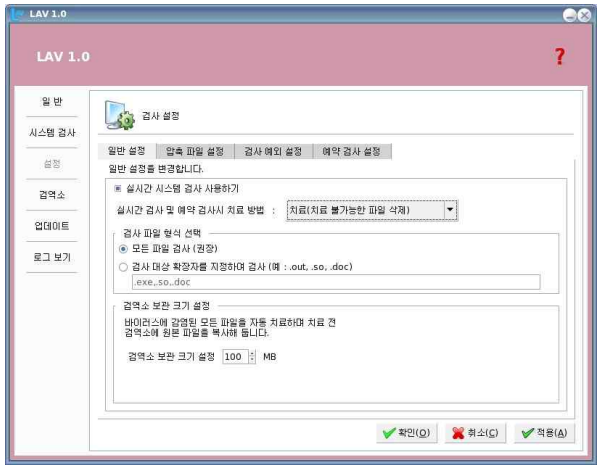
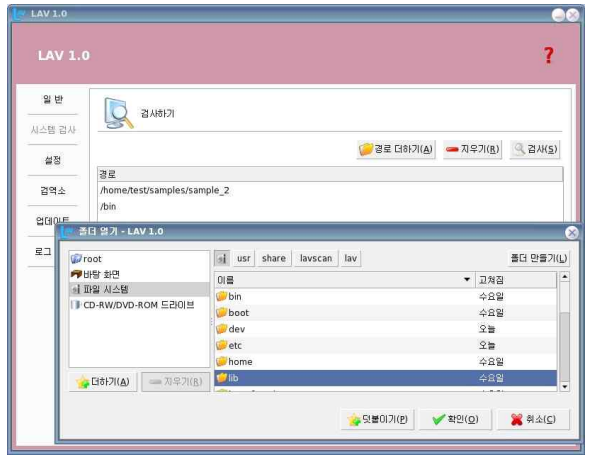
단계	항목/시험/결과	
시험결과	5	3. 검사 주기를 '특정 요일', 시간도 설정하고 '확인'  4. 해당 요일이 아닌 날의 시간에 예약 검사 기능이 수행되지 않는지 확인 

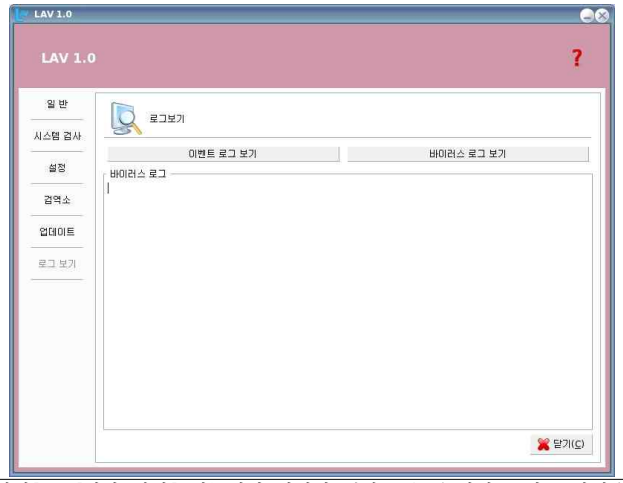
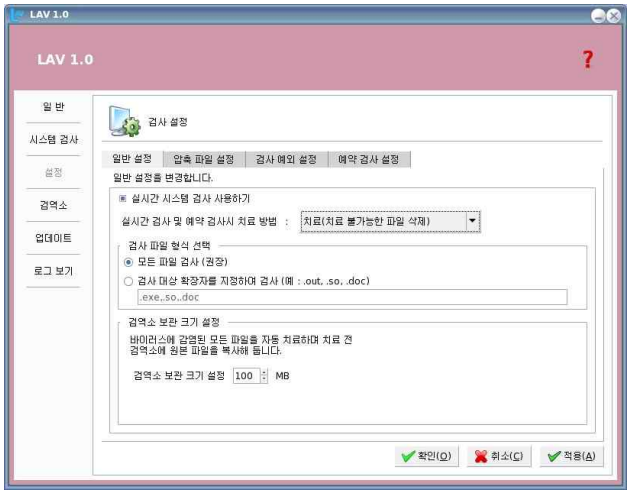
단계	항목/시험/결과	
시험절차	시험항목	LAV 비검사 영역
	1	1. 바이러스 파일을 특정 디렉토리에 저장한다. 2. [설정] > [검사 예외 설정] 메뉴에서 바이러스 파일이 저장된 디렉토리를 추가한다.
	2	1. [설정] > [검사 예외 설정] 메뉴에서 추가한 경로를 활성화 시키고 치료 방법은 '치료(치료 불가능한 파일 삭제)'로 설정한다. 2. 실시간 검사로 바이러스 파일이 검출되지 않는지 확인한다.
	3	1. [설정] > [검사 예외 설정] 메뉴에서 추가한 경로를 활성화 시키고 치료 방법은 '치료(치료 불가능한 파일 삭제)'로 설정한다. 2. [시스템 검사] 메뉴에서 바이러스 파일이 저장된 디렉토리를 추가한다. 3. 검사를 수행한 후 바이러스 파일이 검출되지 않는지 확인한다.
	4	1. [설정] > [검사 예외 설정] 메뉴에서 추가한 경로를 활성화 시키고 치료 방법은 '치료(불가능한 파일 삭제)'로 설정한다. 2. [시스템 검사] 메뉴에서 바이러스 파일이 저장된 디렉토리를 포함한 여러 디렉토리를 추가한다. 3. 검사를 수행한 후 바이러스 파일이 검출되지 않는지 확인한다.
	5	1. [설정] > [검사 예외 설정] 메뉴에서 추가한 경로를 활성화 시키고 치료 방법은 '치료(치료 불가능한 파일 삭제)'로 설정한다. 2. [설정] > [예약 검사 설정] 메뉴에서 바이러스 파일이 저장된 디렉토리를 검사 대상으로 설정하고 예약 검사를 수행한다. 3. 검사를 수행한 후 바이러스 파일이 검출되지 않는지 확인한다.
	6	1. [설정] > [검사 예외 설정] 메뉴에서 추가한 경로를 비활성화 시키고 치료 방법은 '치료(치료 불가능한 파일 삭제)'로 설정한다. 2. 바이러스 파일이 검출되는지 확인한다.
시험결과	1	1. 바이러스 파일을 특정 디렉토리에 저장한다. 

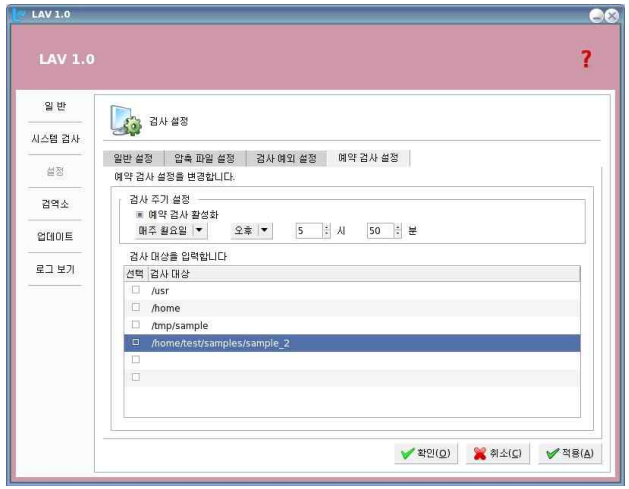
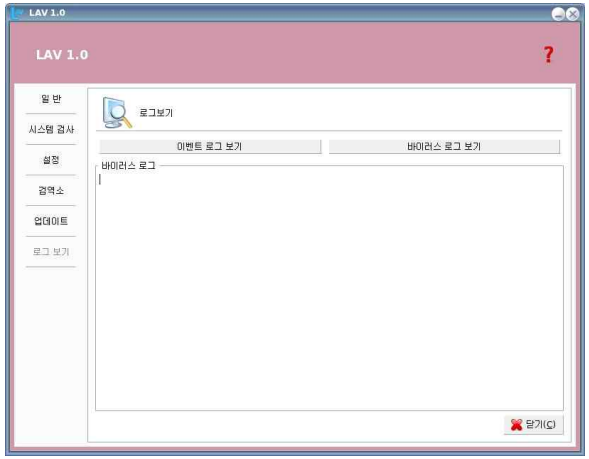
단계		항목/시험/결과
시험결과	1	2. [설정] > [검사 예외 설정] 메뉴에서 바이러스 파일이 저장된 디렉토리 추가 
	2	1. [설정] > [일반 설정] 메뉴에서 실시간 검사를 'On' 시키고 치료 방법은 '치료(치료 불가능한 파일 삭제)'로 설정 

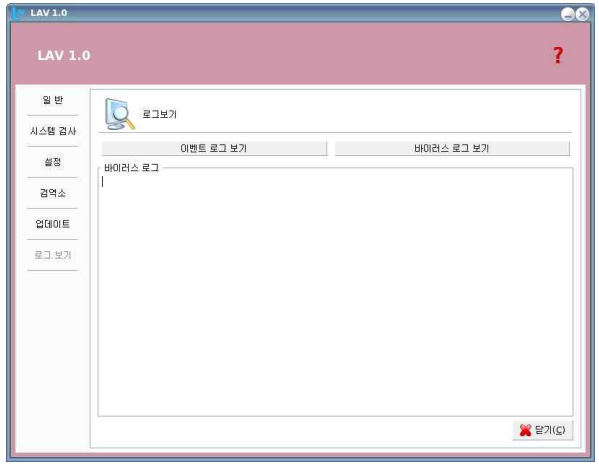
단계		항목/시험/결과
시험결과	2	2. 실시간 검사로 바이러스 파일이 검출되지 않는지 확인 
	3	1. [설정] > [일반 설정] 메뉴에서 실시간 검사를 'On' 시키고 치료 방법은 '치료(치료 불가능한 파일 삭제)'로 설정 

단계	항목/시험/결과	
시험결과	3	2. [시스템 검사] 메뉴에서 바이러스 파일이 저장된 디렉토리 추가  3. 검사를 수행한 후 바이러스 파일이 검출되지 않는지 확인 

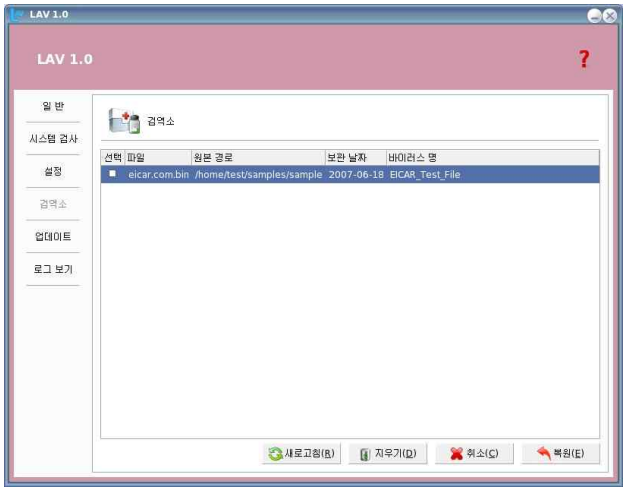
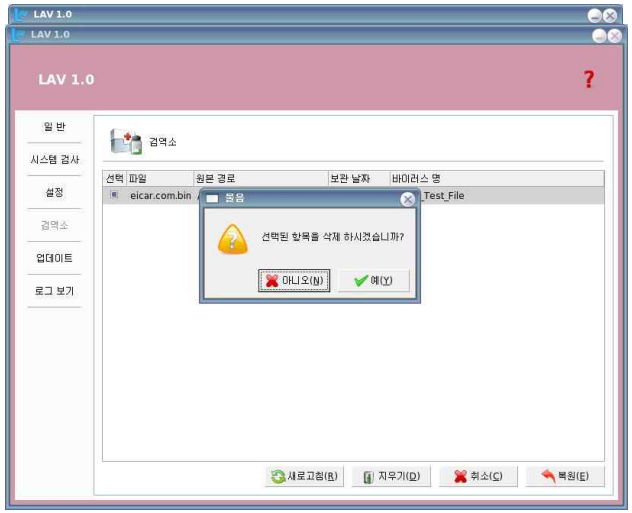
단계	항목/시험/결과	
시험결과	4	1. [설정] > [일반 설정] 메뉴에서 실시간 검사를 'On' 시키고 치료 방법은 '치료(치료 불가능한 파일 삭제)'로 설정  2. [시스템 검사] 메뉴에서 바이러스 파일이 저장된 디렉토리를 포함한 여러 디렉토리 추가 

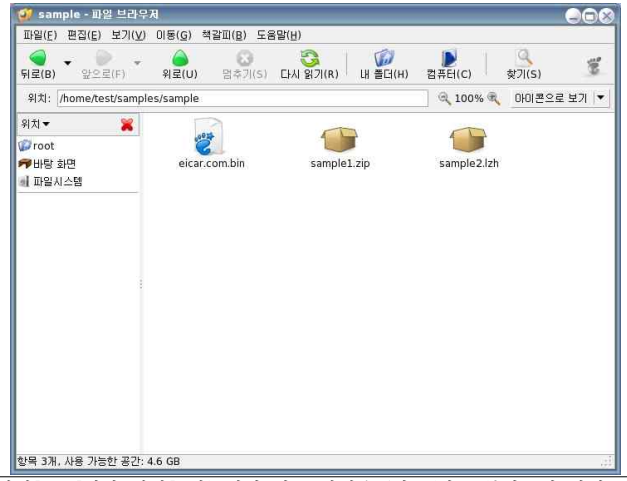
단계		항목/시험/결과
시험결과	4	3. 검사를 수행한 후 바이러스 파일이 검출되지 않는지 확인 
	5	1. [설정] > [일반 설정] 메뉴에서 실시간 검사를 'On' 시키고 치료 방법은 '치료(치료 불가능한 파일 삭제)'로 설정 

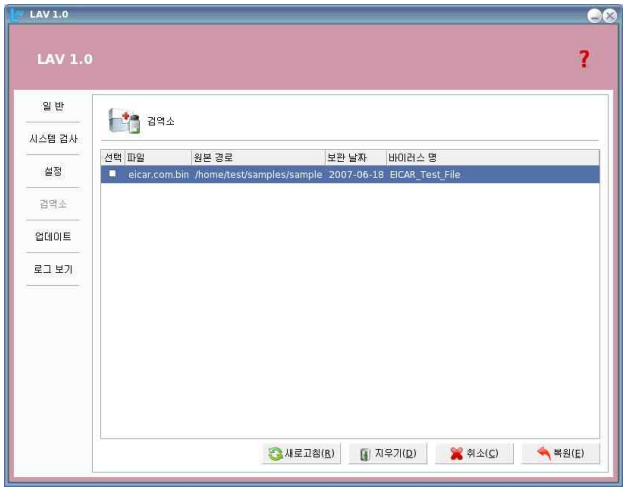
단계		항목/시험/결과
시험결과	5	2. [설정] > [예약 검사 설정] 메뉴에서 바이러스 파일이 저장된 디렉토리를 검사 대상으로 설정하고 예약 검사를 수행한다.  3. 검사를 수행한 후 바이러스 파일이 검출되지 않는지 확인 

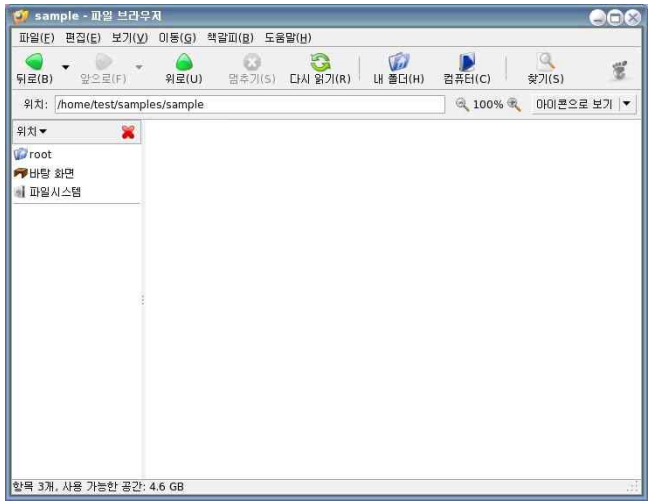
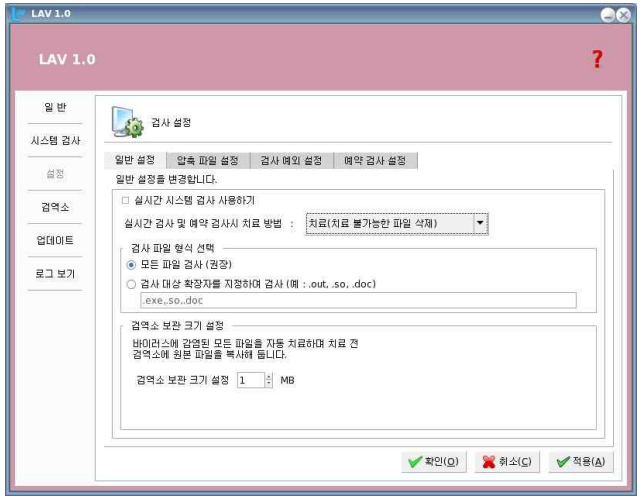
단계	항목/시험/결과	
시험결과	6	1. [설정] > [일반 설정] 메뉴에서 실시간 검사를 'Off' 시키고 치료 방법은 '치료(치료 불가능한 파일 삭제)'로 설정  2. 바이러스 파일이 검출되는지 확인 
비 고		

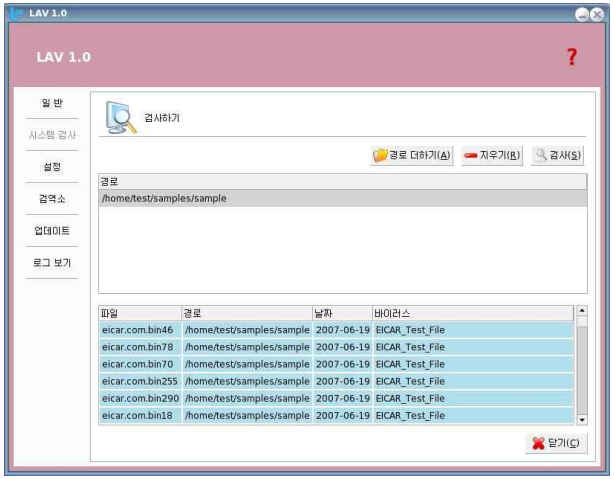
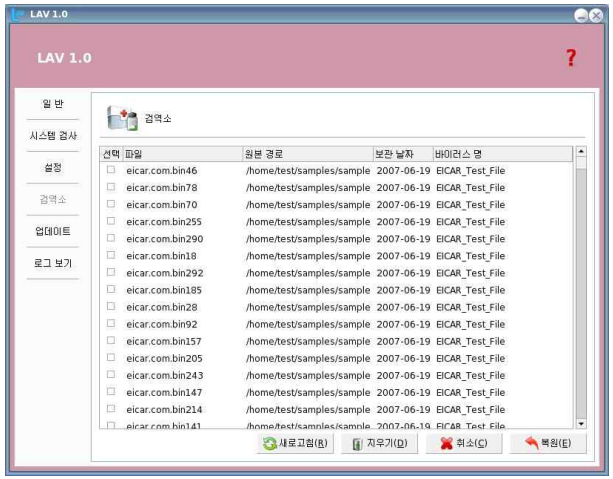
단계	항목/시험/결과	
시험절차	시험항목	LAV 검역소
	1	1. [설정] > [일반 설정] 메뉴에서 치료 방법은 '치료(치료 불가능한 파일 삭제)'로 설정한다. 2. 실시간 검사 후 치료한 파일들이 '검역소'에 저장되었는지 확인한다. 3. 검역소에 저장된 파일 중 일부를 복원 기능을 통해 복원시킨다. 4. 쉘 프롬프트 또는 파일 브라우징을 통하여 해당 경로에 파일이 복구되었는지 확인한다.
	2	1. [설정] > [일반 설정] 메뉴에서 치료 방법은 '치료(치료 불가능한 파일 삭제)'로 설정한다. 2. 실시간 검사 후 치료한 파일들이 '검역소'에 저장되었는지 확인한다. 3. 검역소에 저장된 파일 중 일부를 삭제 기능을 통해 삭제시킨다. 4. 쉘 프롬프트 또는 파일 브라우징을 통하여 파일이 삭제되었는지 확인한다.
	3	1. [설정] > [일반 설정] 메뉴에서 '검역소 보관 크기'를 1MB로 줄인다. 2. 실시간 검사, 시스템 검사 등을 이용하여 바이러스 파일이 1MB 이상이 될 때까지 치료한다. 3. 바이러스 파일들의 총 합계 용량이 검역소 크기보다 커지면 오래된 파일이 삭제되고 최신 파일이 남는지 확인한다.
시험결과	1	1. [설정] > [일반 설정] 메뉴에서 치료 방법을 '치료(치료 불가능한 파일 삭제)'로 설정 

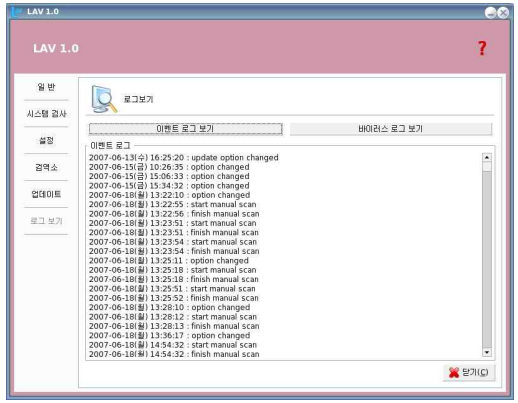
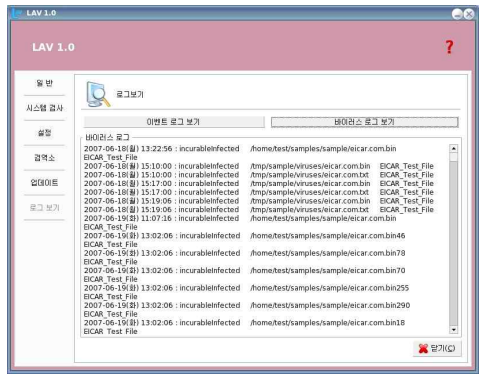
단계	항목/시험/결과	
시험결과	1	2. 실시간 검사 후 치료한 파일들이 '검역소'에 저장되었는지 확인  3. 검역소에 저장된 파일 중 일부를 복원 기능을 통해 복원 

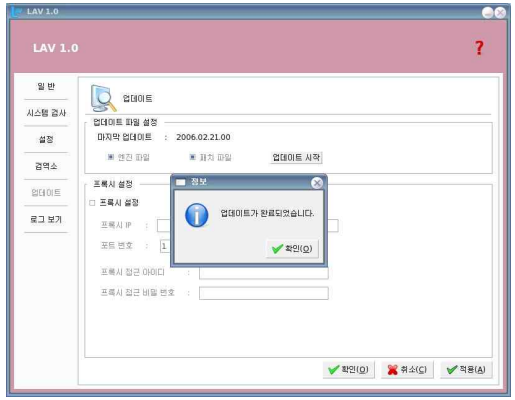
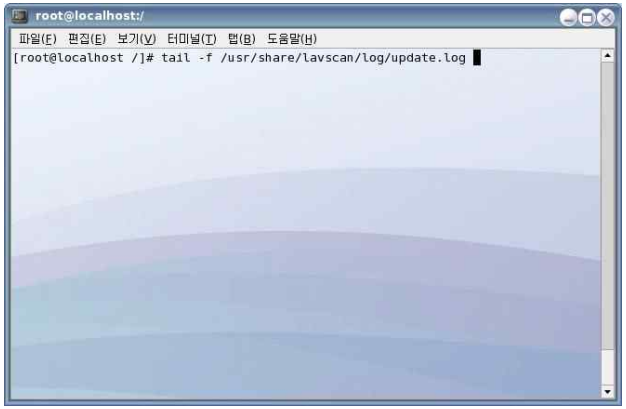
단계	항목/시험/결과	
시험결과	1	4. 쉘 프롬프트 또는 파일 브라우징을 통하여 해당 경로에 파일이 복구되었는지 확인한다. 
	2	1. [설정] > [일반 설정] 메뉴에서 치료 방법은 '치료(치료 불가능한 파일 삭제)'로 설정 

단계	항목/시험/결과	
시험결과	2	2. 실시간 검사 후 치료한 파일들이 '검역소'에 저장되었는지 확인  3. 검역소에 저장된 파일 중 일부를 삭제 기능을 통해 삭제

단계	항목/시험/결과	
시험결과	2	4. 쉘 프롬프트 또는 파일 브라우징을 통하여 해당 경로에 파일이 삭제되었는지 확인 
	3	1. [설정] > [일반 설정] 메뉴에서 '검역소 보관 크기'를 1MB로 줄인다. 

단계	항목/시험/결과	
시험결과	3	2. 실시간 검사, 시스템 검사 등을 이용하여 바이러스 파일이 1MB 이상이 될 때까지 치료  3. 바이러스 파일들의 총 합계 용량이 검역소 크기보다 커지면 오래된 파일이 삭제되고 최신 파일이 남는지 확인 

단계	항목/시험/결과	
시험절차	시험항목	로그 보기
	1	1. [로그 보기] 메뉴에서 [이벤트 로그 보기]를 누른다. 2. 이벤트 로그가 시간 순서대로 디스플레이 되는지 확인한다.
	2	1. [로그 보기] 메뉴에서 [바이러스 로그 보기]를 누른다. 2. 바이러스 로그가 시간 순서대로 디스플레이 되는지 확인한다.
시험결과	1	1. [로그 보기] 메뉴에서 [이벤트 로그 보기] 선택하고, 이벤트 로그가 시간 순서대로 디스플레이 되는지 확인 
	2	1. [로그 보기] 메뉴에서 [바이러스 로그 보기] 선택하고, 바이러스 로그가 시간 순서대로 디스플레이 되는지 확인 
비 고		

단계	항목/시험/결과	
시험절차	시험항목	LAV 업데이트
	1	1. [업데이트] 메뉴에서 '업데이트 시작' 을 눌러 업데이트 시킨다. 2. 업데이트가 완료되었다는 창이 뜨는지 확인한다. 3. 터미널을 이용하여 업데이트 로그를 확인한다.
시험결과	1	1. [업데이트] 메뉴에서 '업데이트 시작' 을 눌러, 완료 팝업 확인  2. 터미널을 실행시키고, /usr/share/lavscan/log/update.log 파일을 열어 업데이트된 로그를 확인한다. 
비 고		