

리눅스 PC보안용 LAV 베타테스트  
(한소프트리눅스) 기능 테스트 절차서

한국소프트웨어진흥원  
공개SW기술지원센터

## <Revision 정보>

일자	VERSION	변경내역	작성자
2007. 1.22	0.1	초기 작성	양선주

# 목 차

1. 문서 개요 .....	4
가. 문서의 목적 .....	4
나. 본 문서의 사용방법 .....	4
2. 테스트 절차 내역 .....	5
가. LAV 기동 테스트 .....	5
나. LAV 기능 테스트 .....	7

## 1. 문서 개요

본 문서는 리눅스 PC보안용 솔루션인 LAV를 Haansoft Linux 2006 Workstation OS에서 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 Haansoft Linux 2006 Workstation OS 호환성 결과
- 리눅스 PC보안 솔루션 LAV와 Haansoft Linux 2006 Workstation OS 기능성 결과
- 진행 중 문제 발생 사항과 각각의 진행사항

### 나. 본 문서의 사용방법

다음과 같은 방법으로 사용할 수 있다.

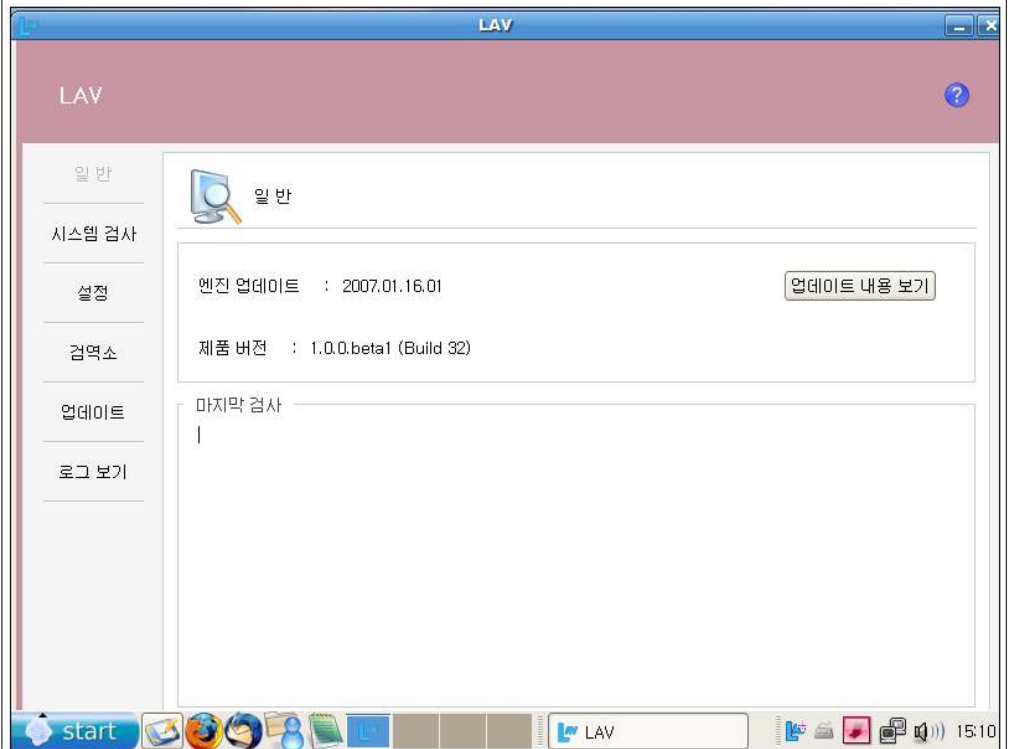
- 리눅스 PC보안 솔루션 LAV와 Haansoft Linux 2006 Workstation OS의 호환성 결과를 확인한다.
- Haansoft Linux 2006 Workstaion OS에서 LAV의 설치, 구동 및 기능 실행 결과를 확인한다.

## 2. 테스트 절차 내역

### 가. LAV 기동 테스트

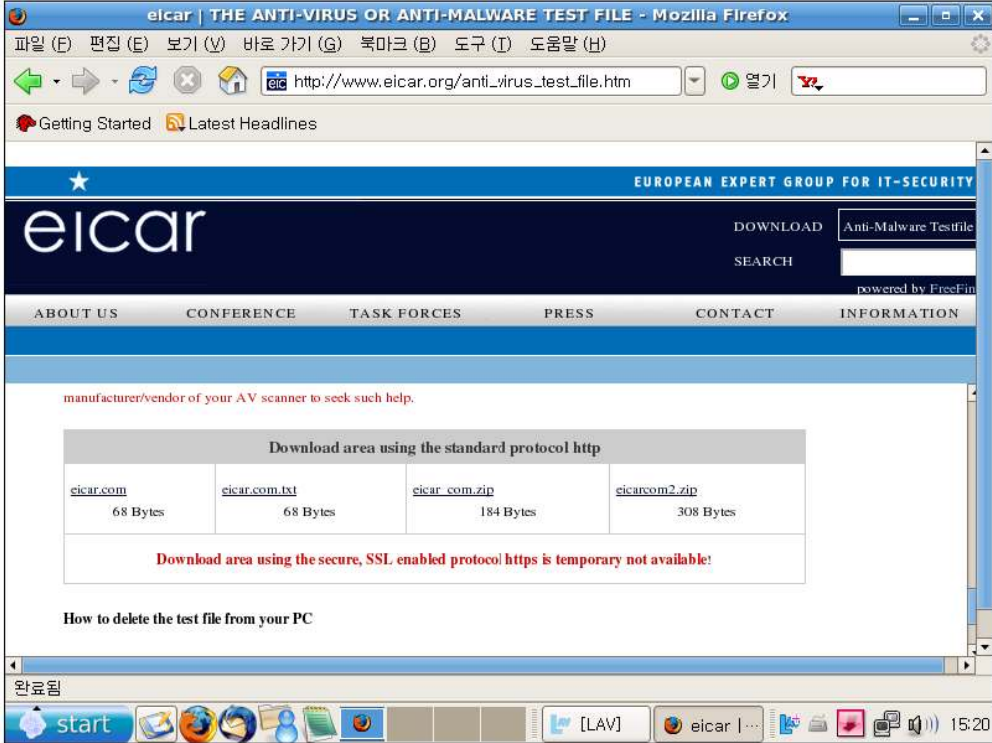
단계	항목/시험/결과	
1	시험항목	LAV 기동 확인
	시험절차	1. X-windows로 로그인 2. 시작메뉴의 프로그램 실행바를 이용하여 실행 3. 기동 확인
	시험결과	1. X-windows로 로그인 후, 시작메뉴의 프로그램 실행바를 이용하여 실행한다. 

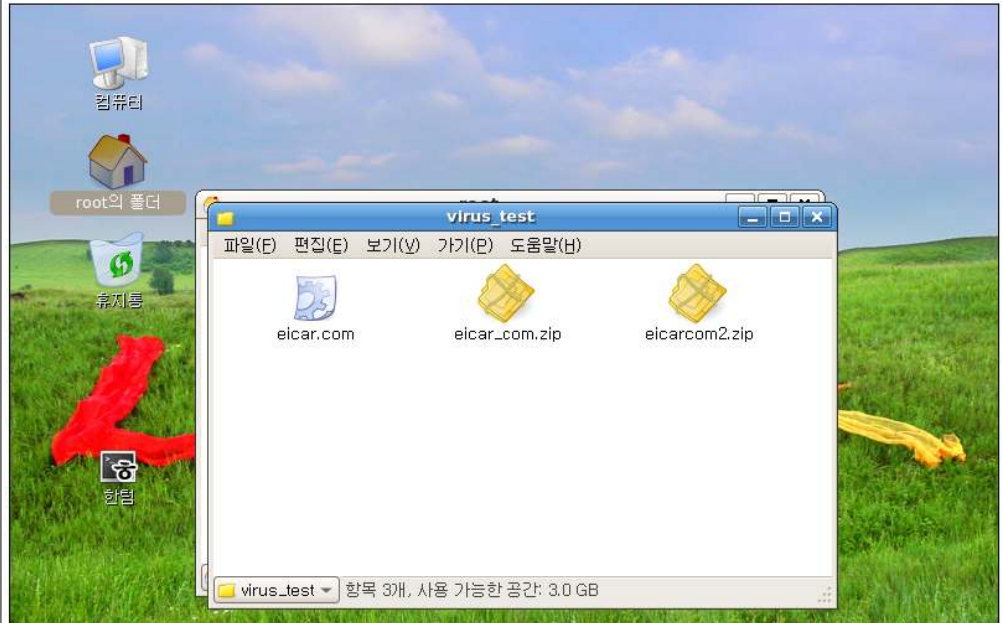
2. 가동되는 것을 확인한다.



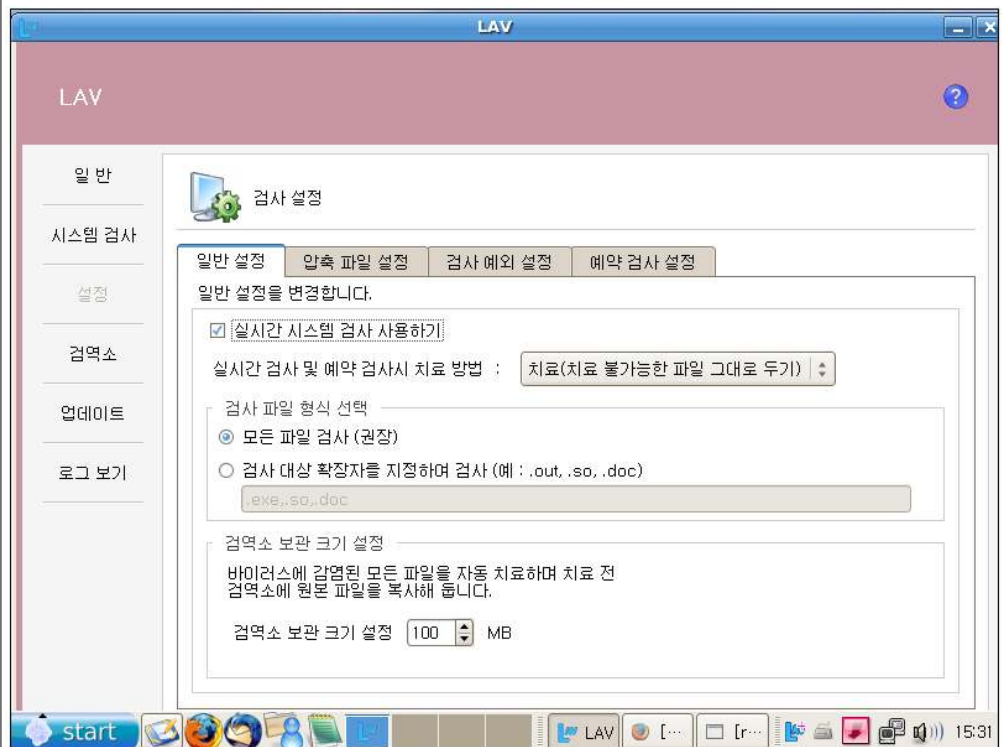
비 고

## 나. LAV 기능 테스트

단계	항목/시험/결과	
hr11	시험항목	LAV의 실시간 검사
	시험절차	<ol style="list-style-type: none"> <li>1. <a href="http://www.eicar.org/anti_virus_test_file.htm">http://www.eicar.org/anti_virus_test_file.htm</a> 에서 바이러스 샘플파일을 다운로드 하여 해당 시스템에 저장한다.</li> <li>2. [설정] 메뉴에서 '실시간 시스템 검사 사용하기' 가 On 되어 있는지 확인하고, 만일 Off 이면 On 시킨다.</li> <li>3. 상기의 URL에서 다운로드한 파일을 저장한 디렉토리로 이동하여 해당 파일을 선택하여 접근이 가능한지 확인한다.</li> <li>4. 셸프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인한다.</li> <li>5. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.</li> </ol>
	시험결과	<ol style="list-style-type: none"> <li>1. <a href="http://www.eicar.org/anti_virus_test_file.htm">http://www.eicar.org/anti_virus_test_file.htm</a>에서 바이러스 샘플파일 다운로드</li> </ol> 

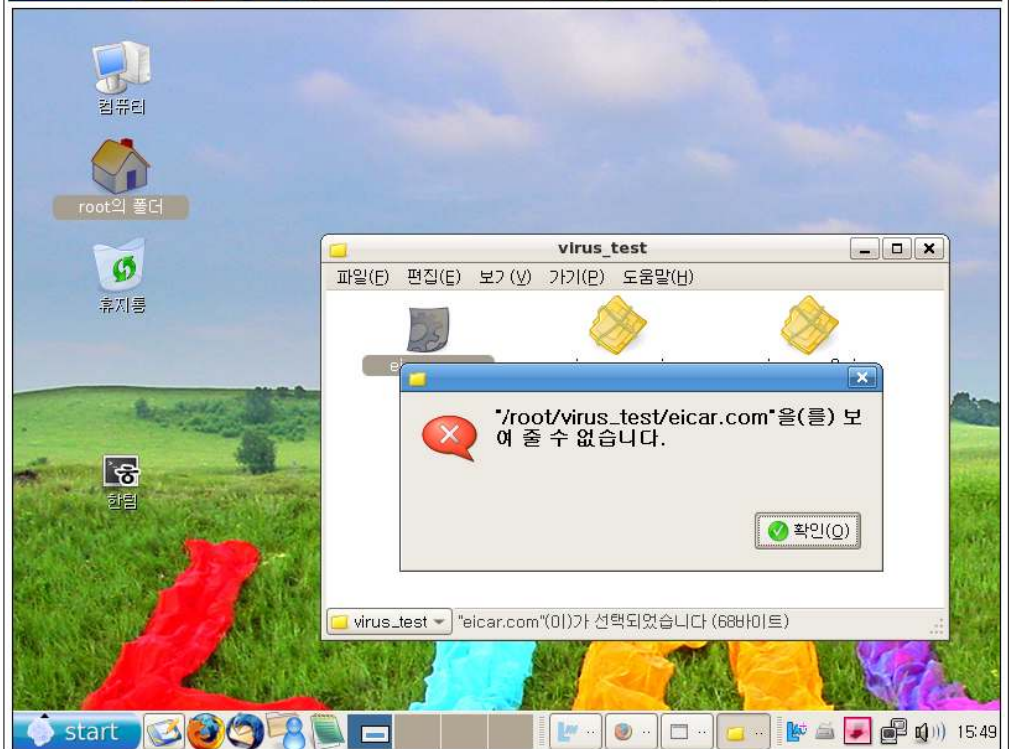
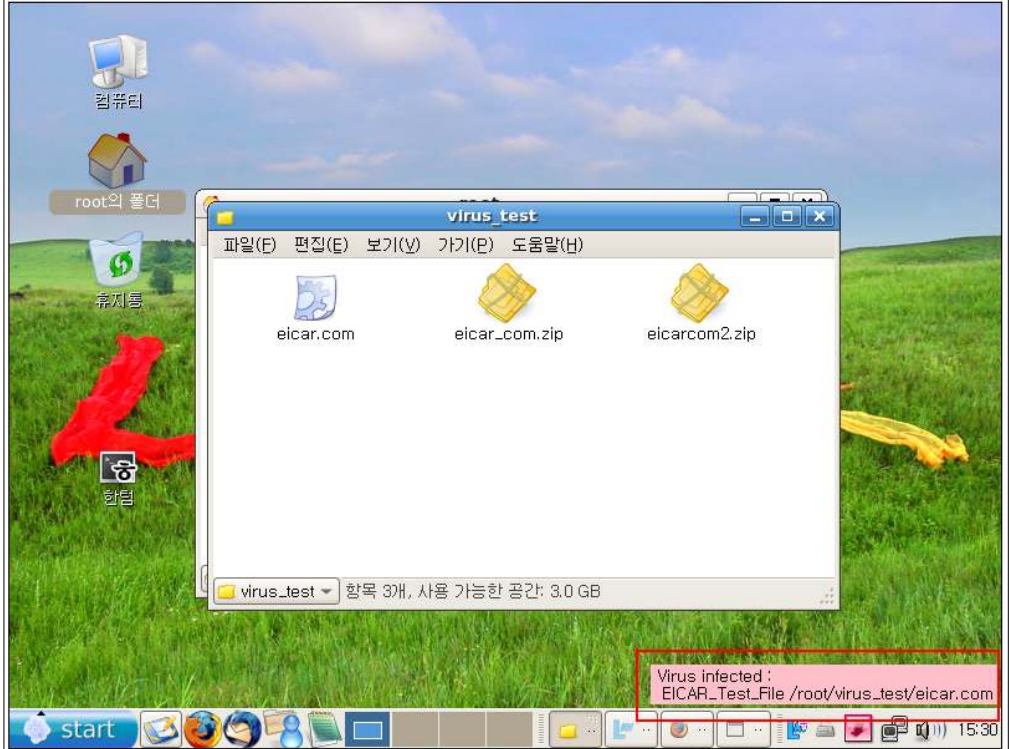


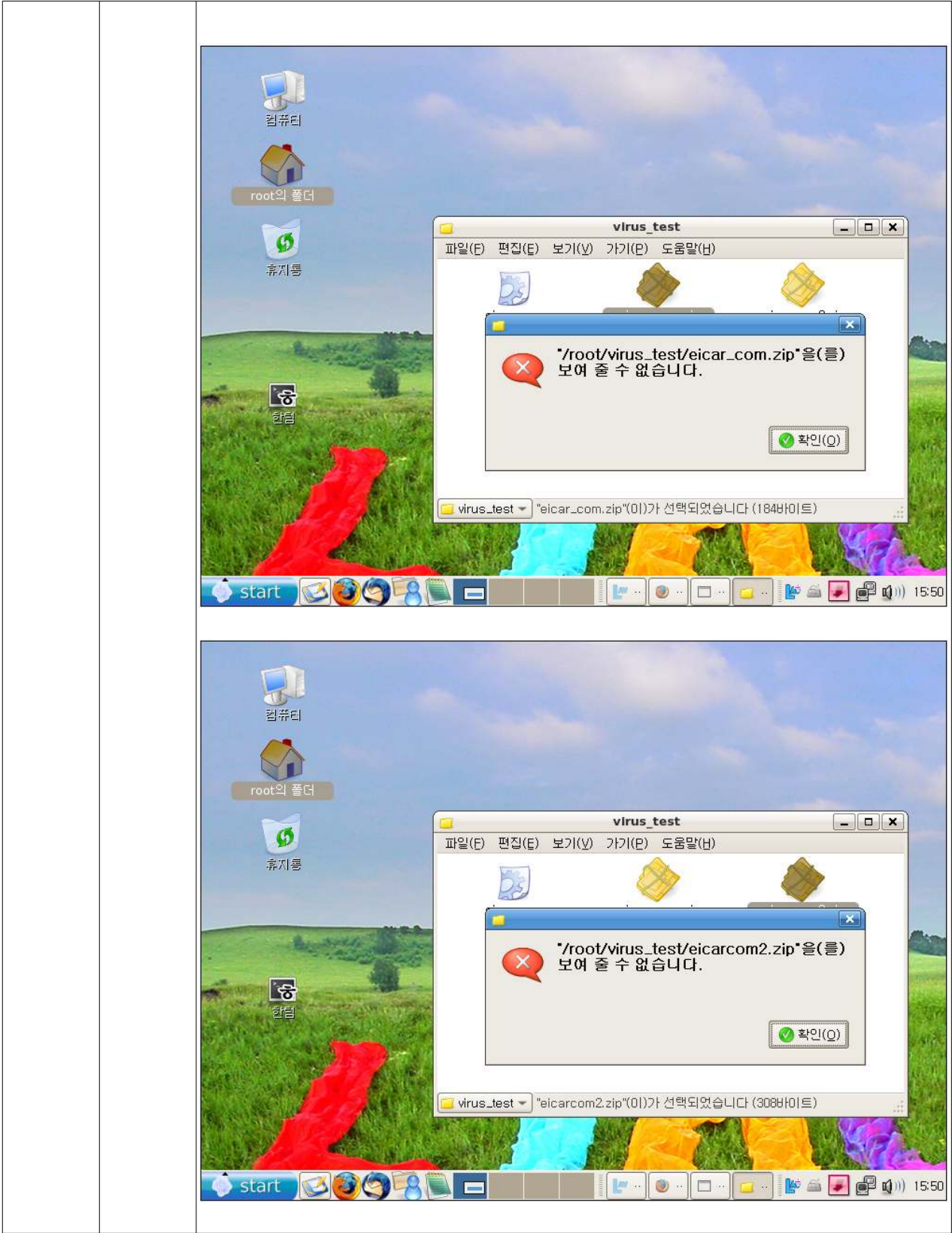
2. [설정] 메뉴에서 '실시간 시스템 검사 사용하기' 가 On 되어 있는지 확인하고, 만일 Off 이면 On 시킨다.





3. 상기의 URL에서 다운로드한 파일을 저장한 디렉토리로 이동하여 해당 파일을 선택하여 접근이 가능한지 확인





## 4. 셸프롬프트에서 해당 파일을 열어, 접근이 가능한지 확인

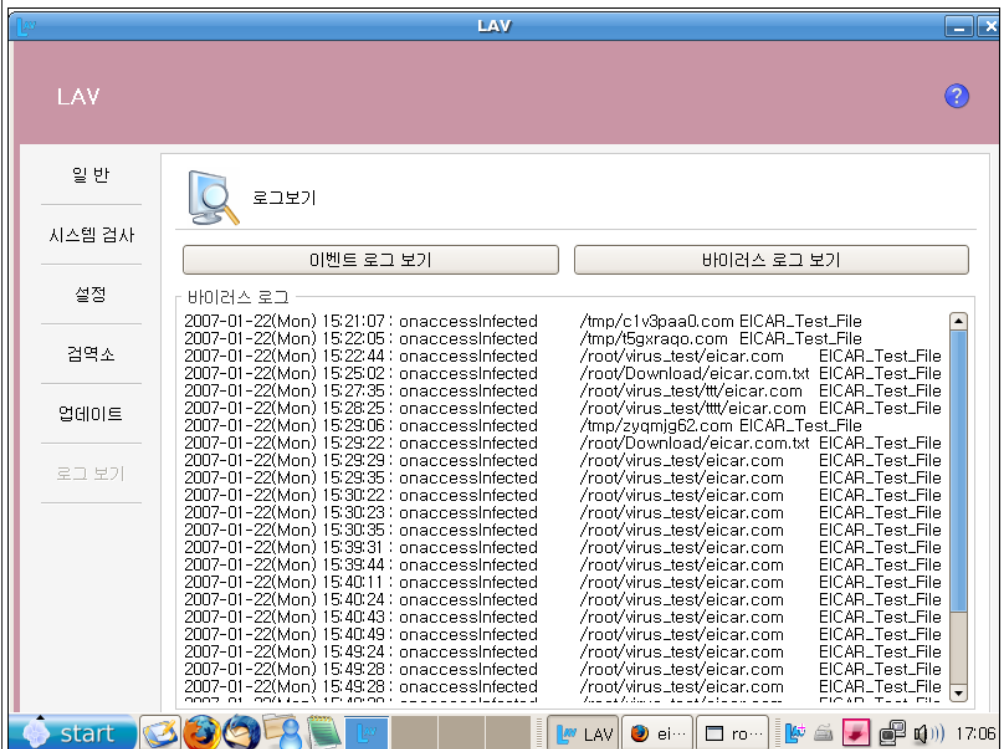
```

[root@test1 ~]# cd virus_test
[root@test1 virus_test]# ls -al
total 24
drwxr-xr-x  2 root root 4096 Jan 22 15:29 .
drwxr-x--- 26 root root 4096 Jan 22 15:41 ..
-rw-r--r--  1 root root   68 Jan 22 15:29 eicar.com
-rw-r--r--  1 root root  184 Jan 22 15:29 eicar_com.zip
-rw-r--r--  1 root root  308 Jan 22 15:29 eicarcom2.zip
[root@test1 virus_test]# cat eicar.com
cat: eicar.com: Operation not permitted
[root@test1 virus_test]# mkdir 1
[root@test1 virus_test]# mv eicar_com.zip test_zip/
[root@test1 virus_test]# cd 1
[root@test1 virus_test]# ls
eicar_com.zip
[root@test1 1]# unzip eicar_com.zip
Archive:  eicar_com.zip
  extracting: eicar.com
[root@test1 1]# ls -al
total 16
drwxr-xr-x  2 root root 4096 Jan 22 15:56 .
drwxr-xr-x  3 root root 4096 Jan 22 15:56 ..
-rw-r--r--  1 root root   68 May 24  2000 eicar.com
-rw-r--r--  1 root root  184 Jan 22 15:29 eicar_com.zip
[root@test1 1]# more eicar.com
more: eicar.com: Operation not permitted
[root@test1 1]# cd ../
[root@test1 virus_test]# mkdir test_zip2
[root@test1 virus_test]# mv eicarcom2.zip 2/
[root@test1 2]# ls
eicarcom2.zip
[root@test1 2]# unzip eicarcom2.zip
Archive:  eicarcom2.zip
  extracting: eicar_com.zip
[root@test1 2]# ls -al

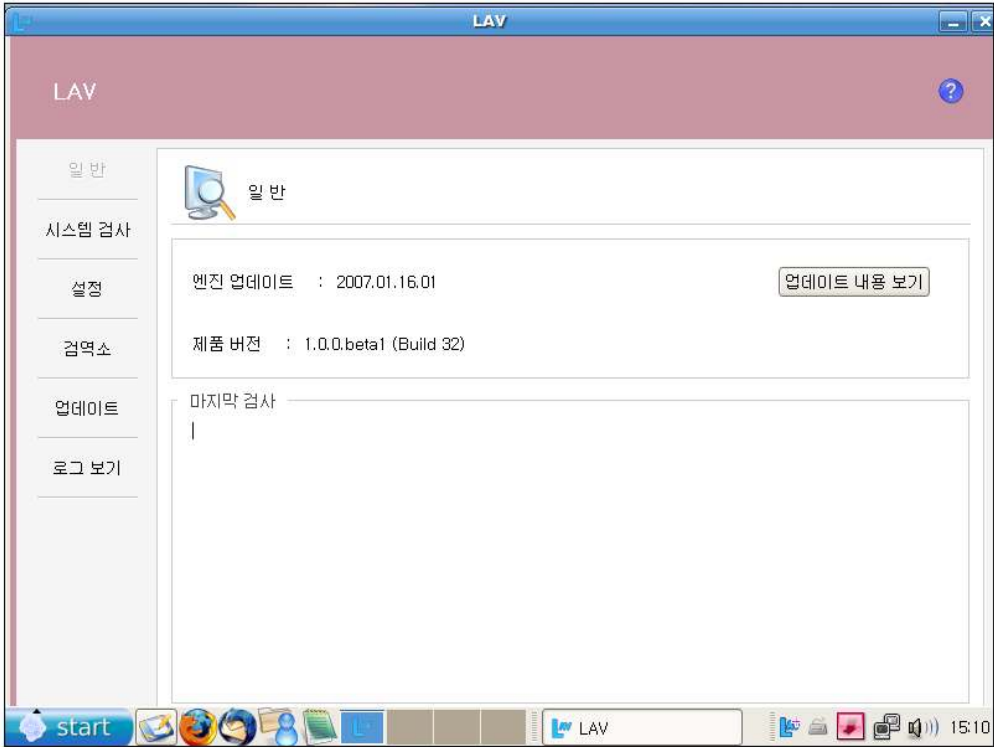
```

```
total 16
drwxr-xr-x 2 root root 4096 Jan 22 15:57 .
drwxr-xr-x 4 root root 4096 Jan 22 15:57 ..
-rw-rw-rw- 1 root root 184 Jul 11 2000 eicar_com.zip
-rw-r--r-- 1 root root 308 Jan 22 15:29 eicarcom2.zip
[root@test1 2]# more eicar.com
more: eicar.com: Operation not permitted
```

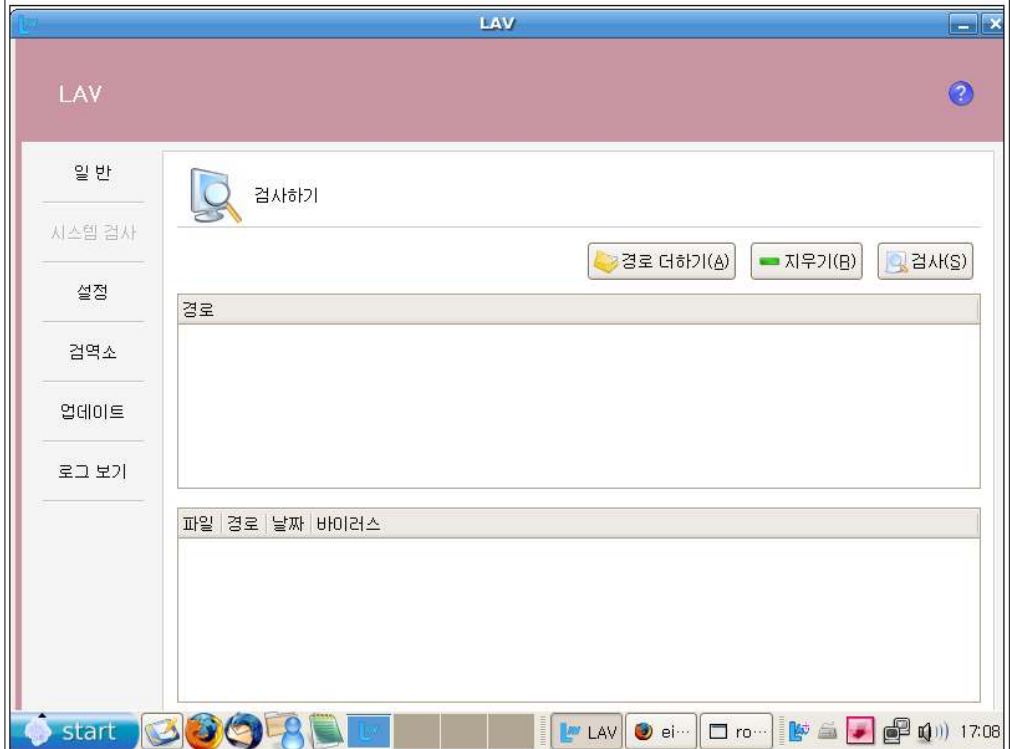
5. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인



비 고

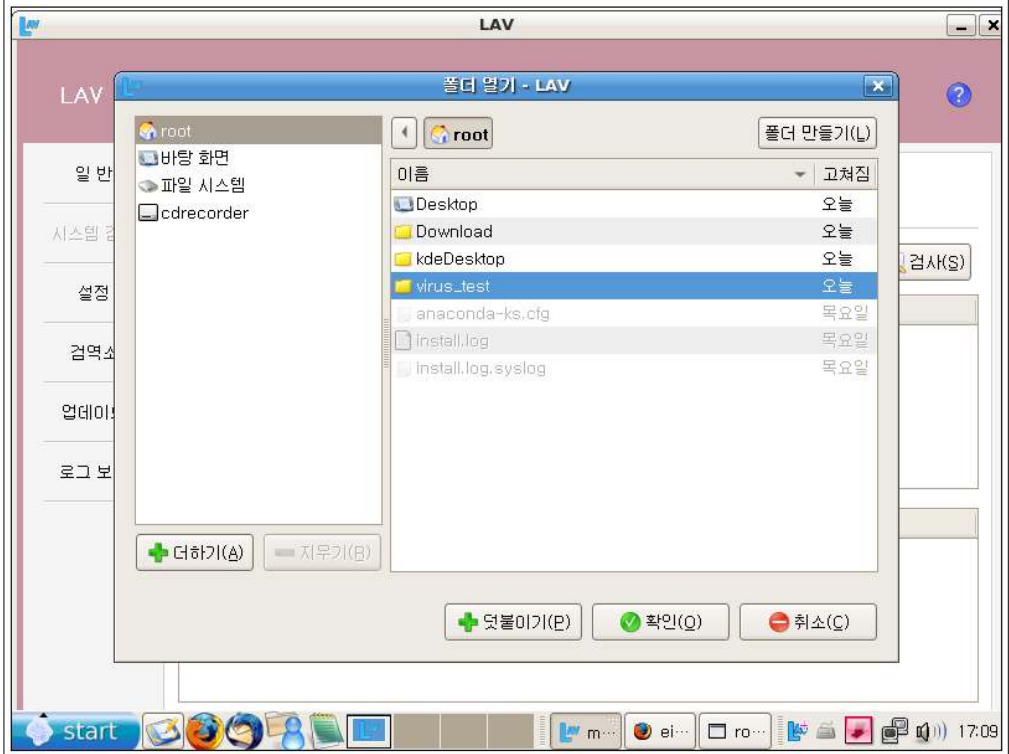
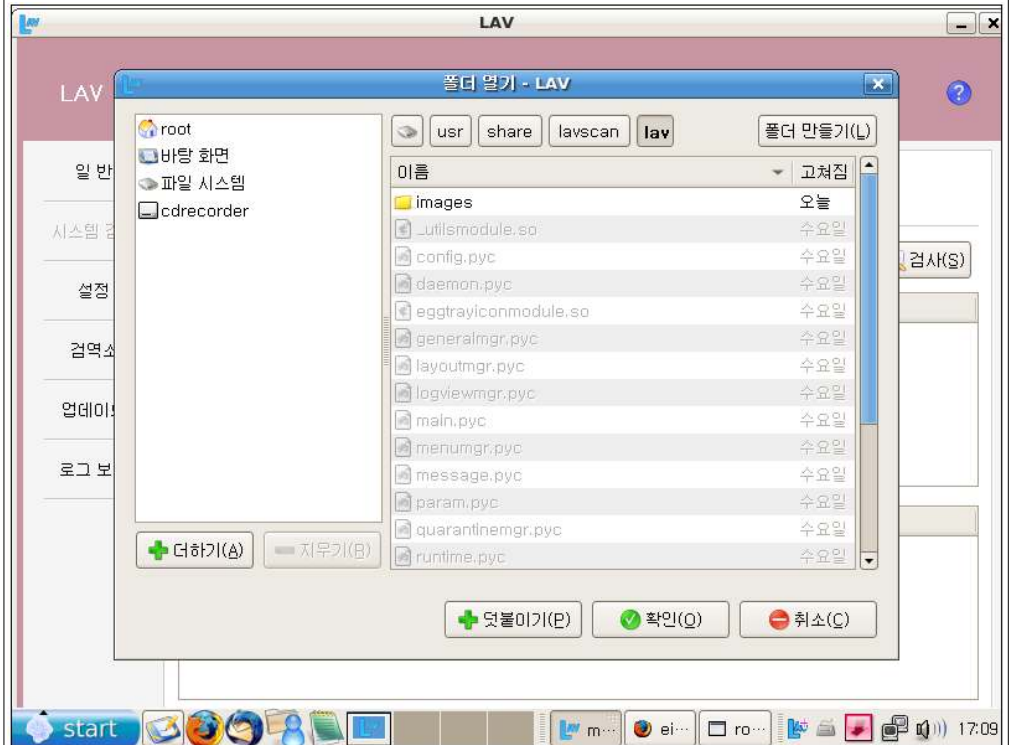
단계	항목/시험/결과	
1	시험항목	LAV의 수동 검사
	시험절차	1. X-windows로 로그인한 후, LAV를 실행시킨다. 2. [시스템 검사] 메뉴를 선택한다. 3. '경로 더하기'를 선택하여 검사하고자 하는 디렉토리를 추가한다. 4. 검사를 실행한다. 5. 결과 화면을 확인한다. 6. [로그보기] 메뉴에서 '바이러스 로그 보기'를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인한다.
	시험결과	1. X-windows로 로그인한 후, LAV 실행 

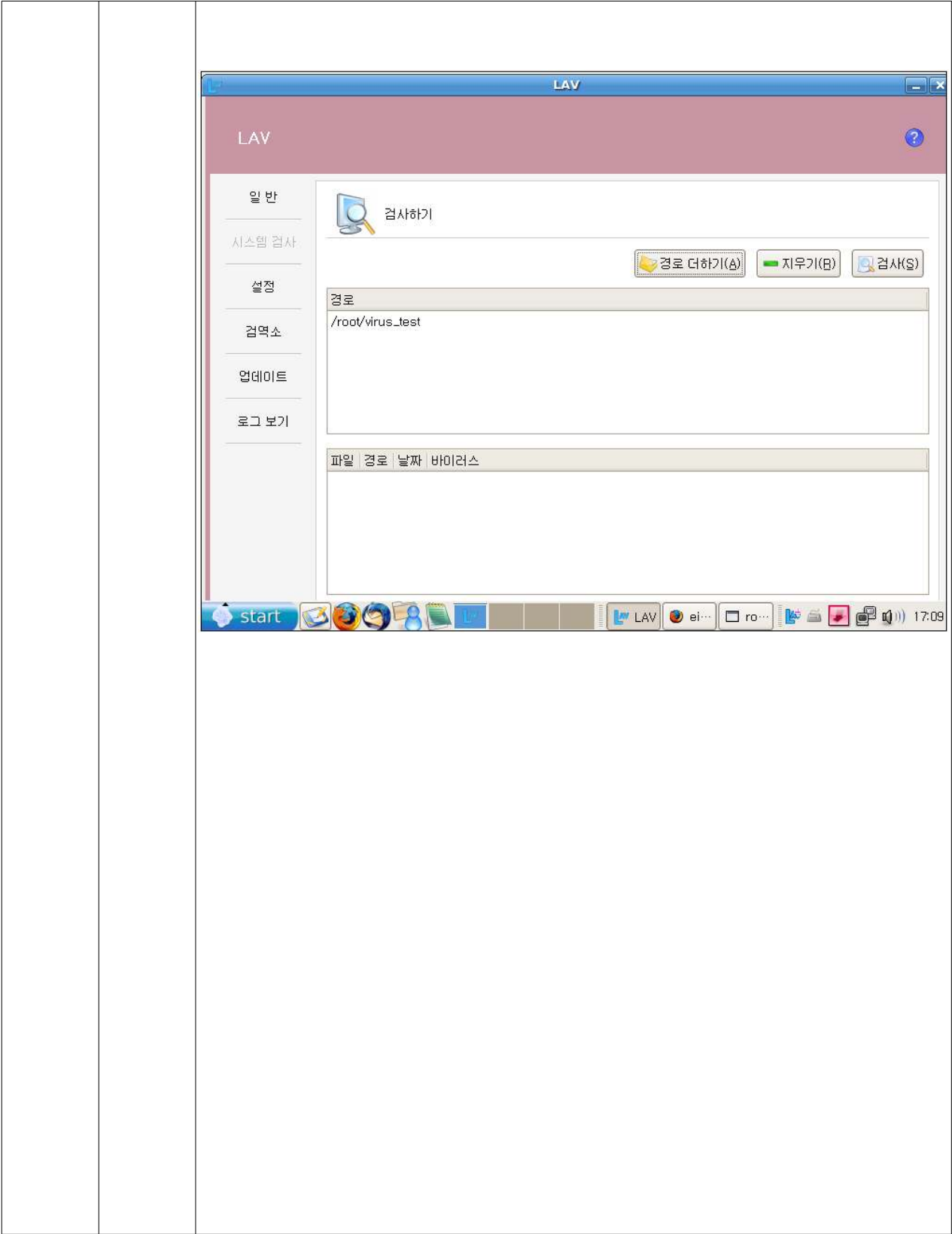
2. [시스템 검사] 메뉴 선택





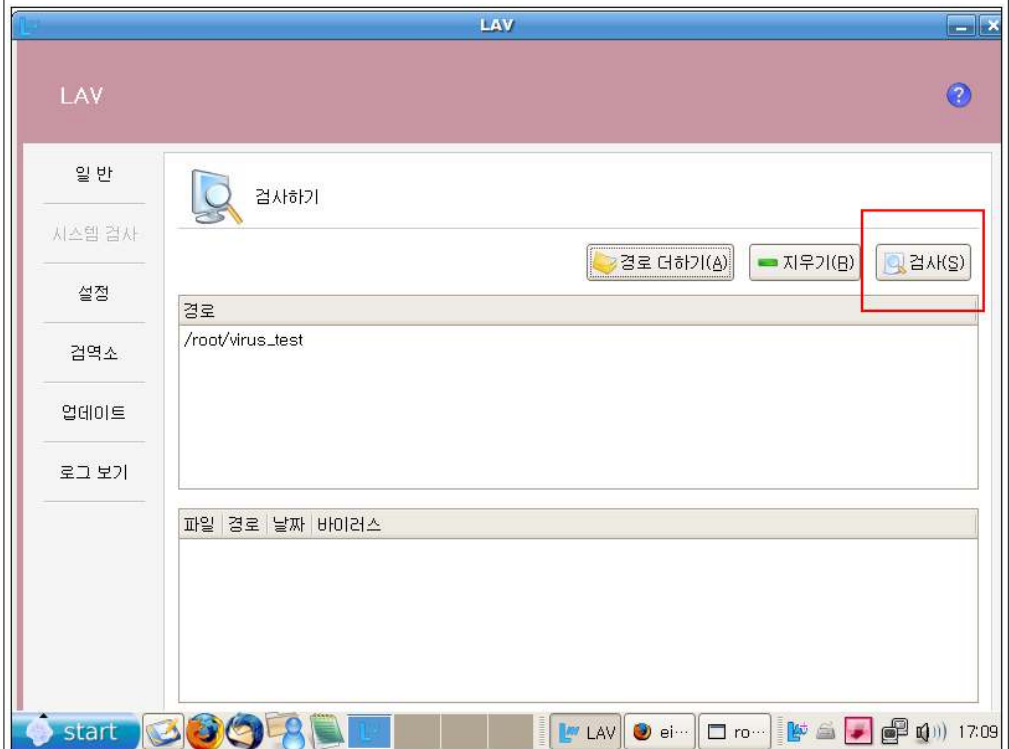
3. '경로 더하기'를 선택하여 검사하고자 하는 디렉토리 추가



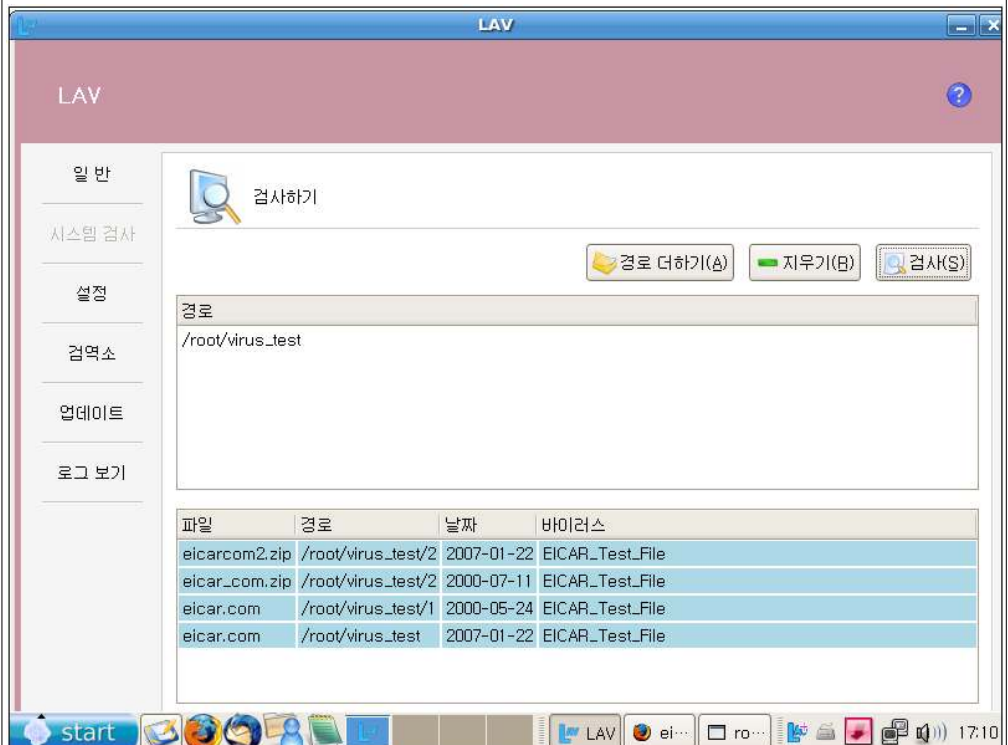
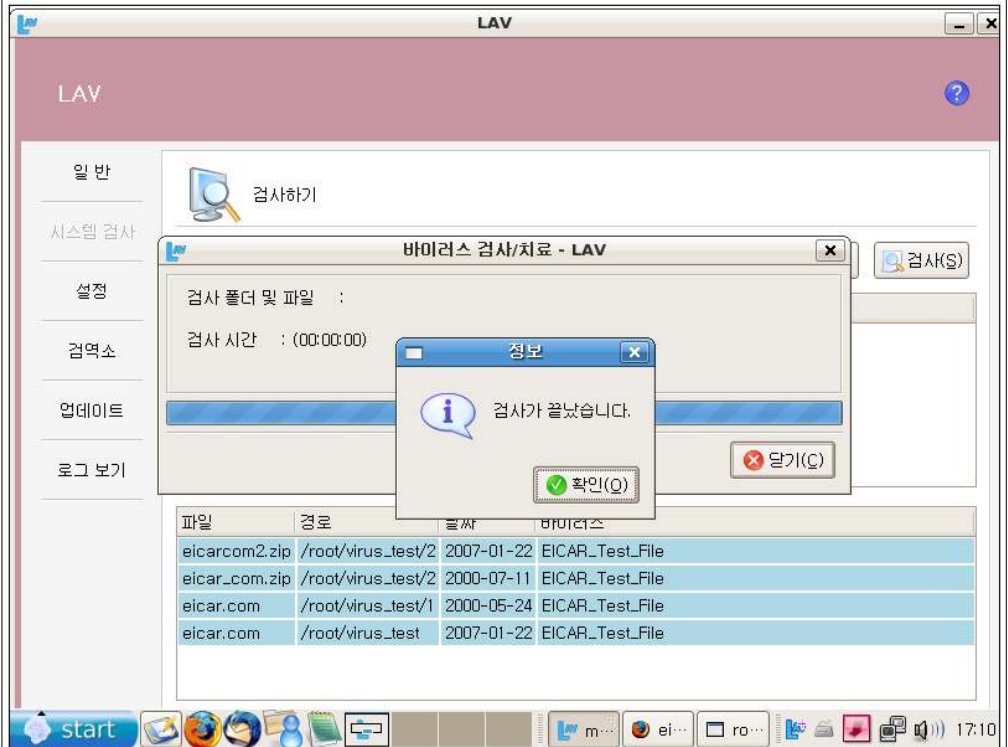




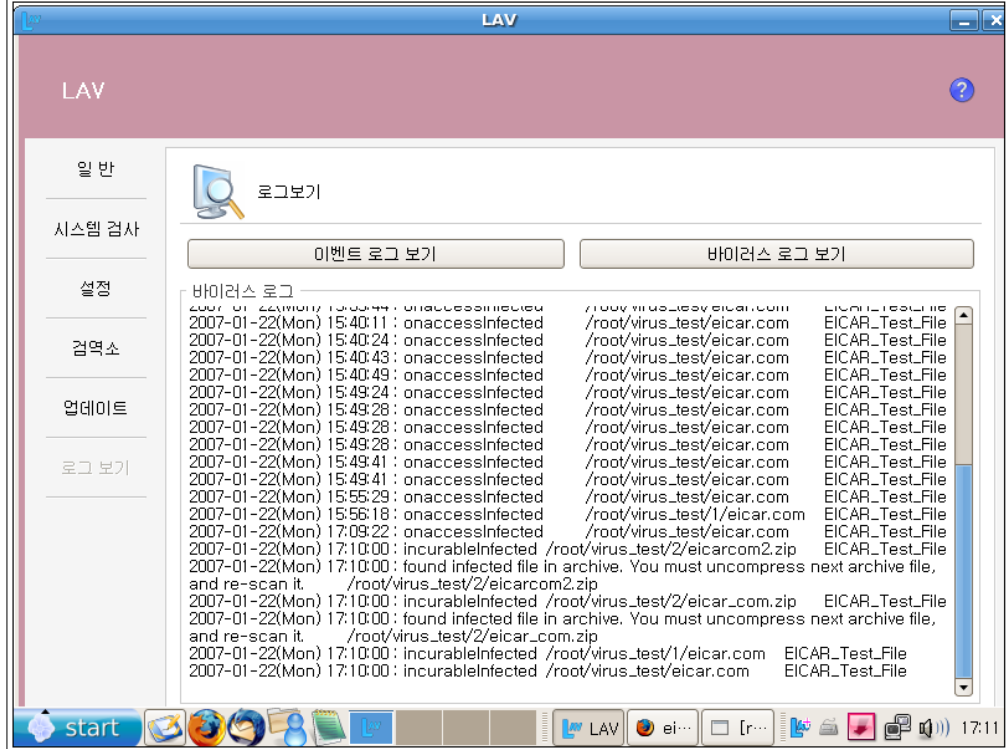
4. 검사를 실행한다.



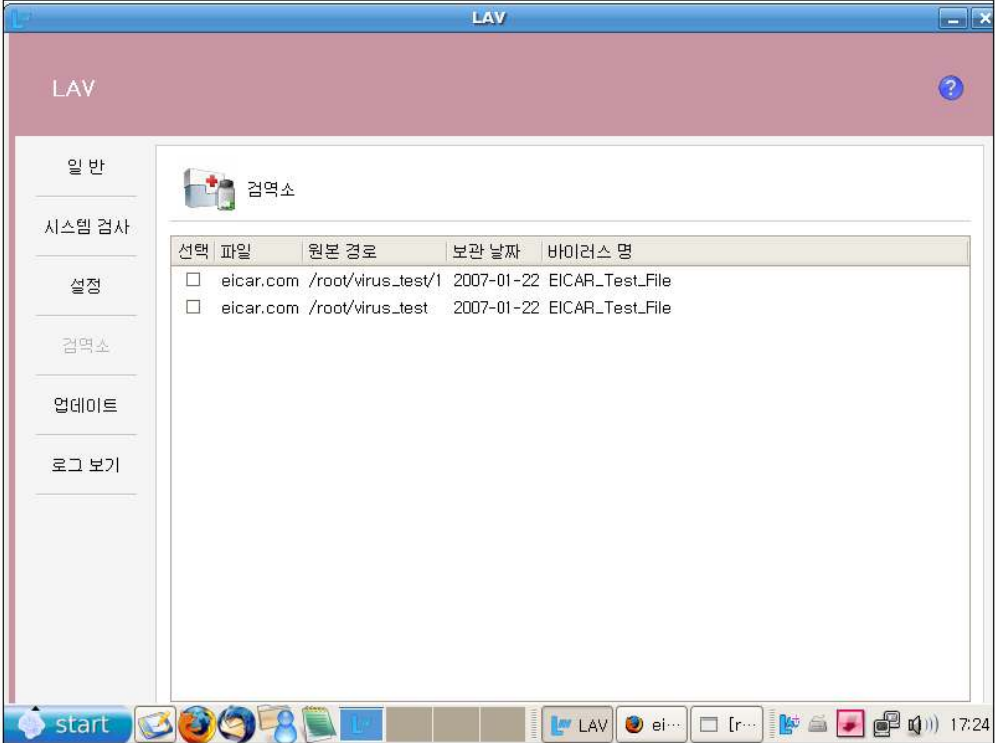
5. 결과 화면을 확인한다.



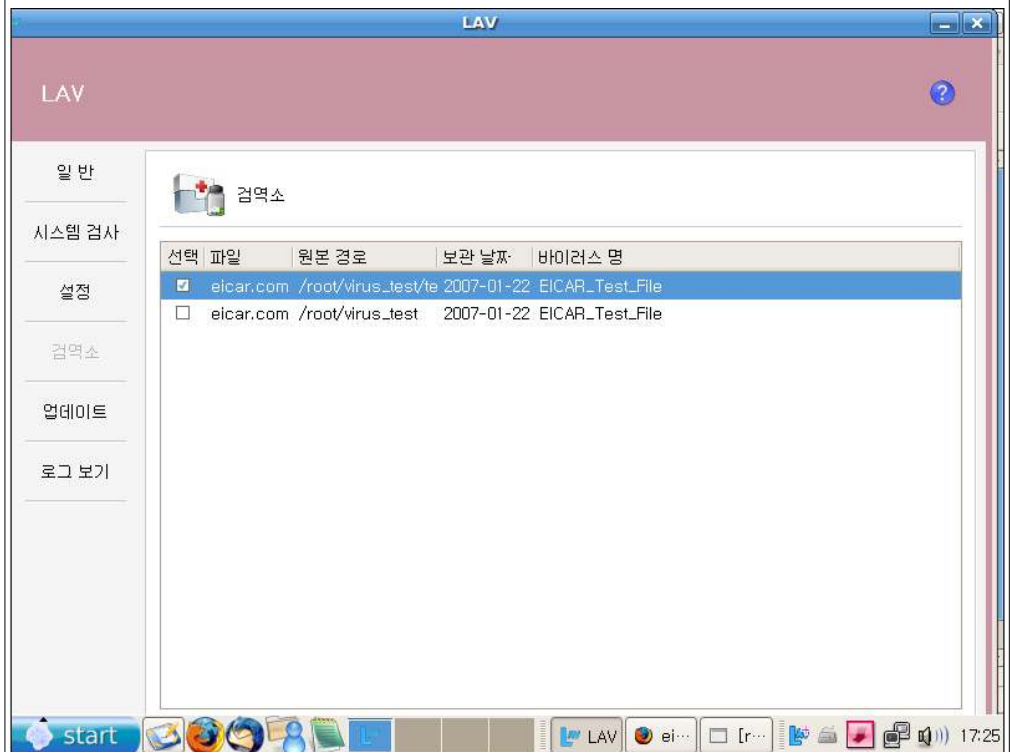
6. [로그보기] 메뉴에서 ‘바이러스 로그 보기’를 선택하여 접근한 바이러스 파일에 대한 로그가 기록되었는지 확인

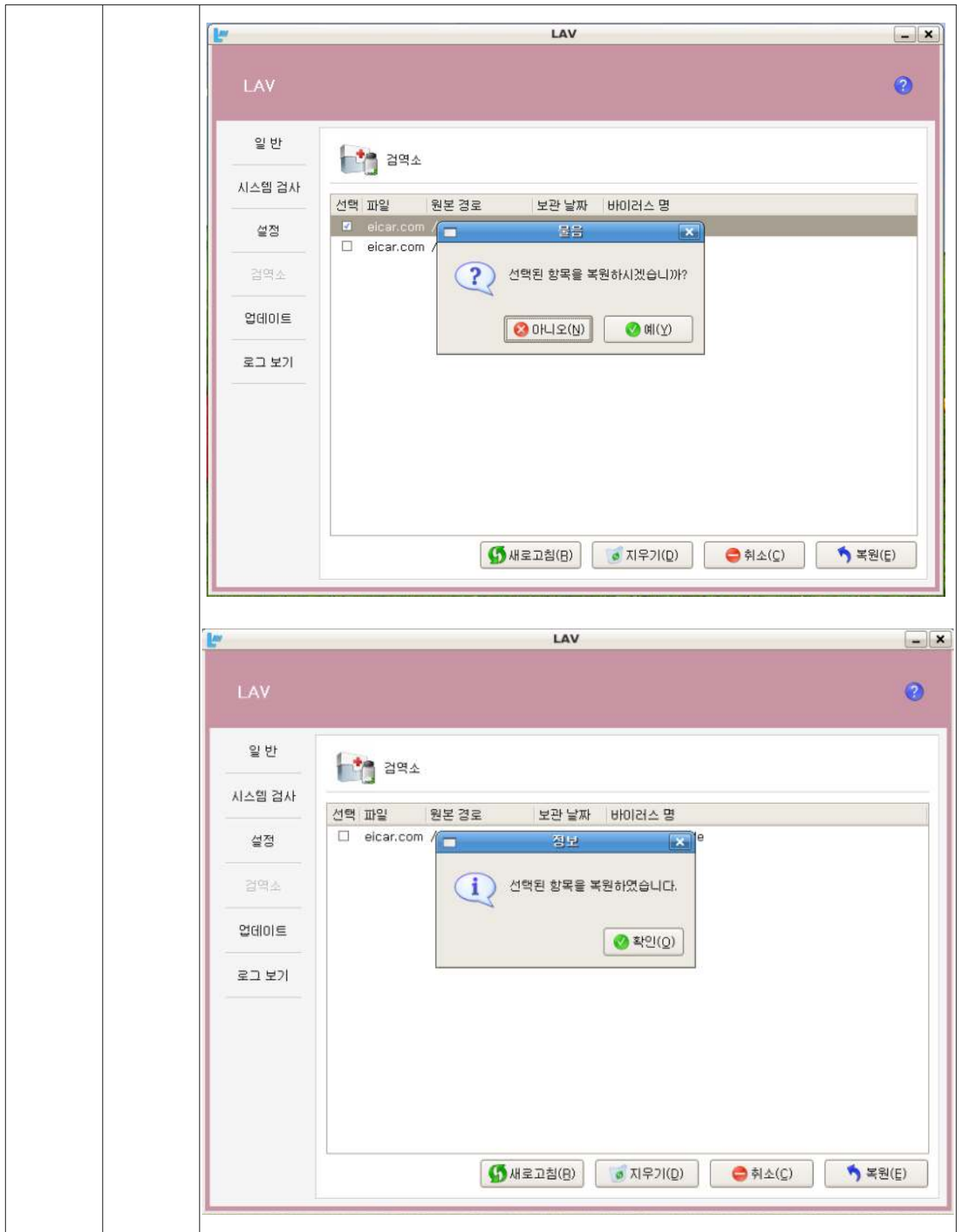


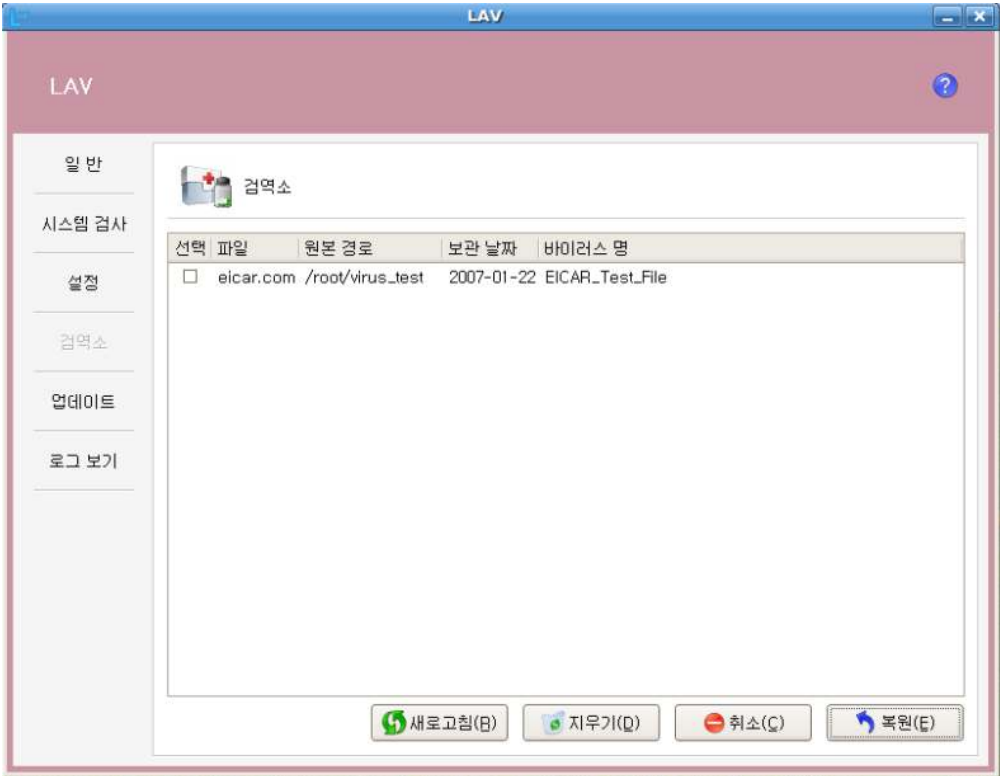
비 고

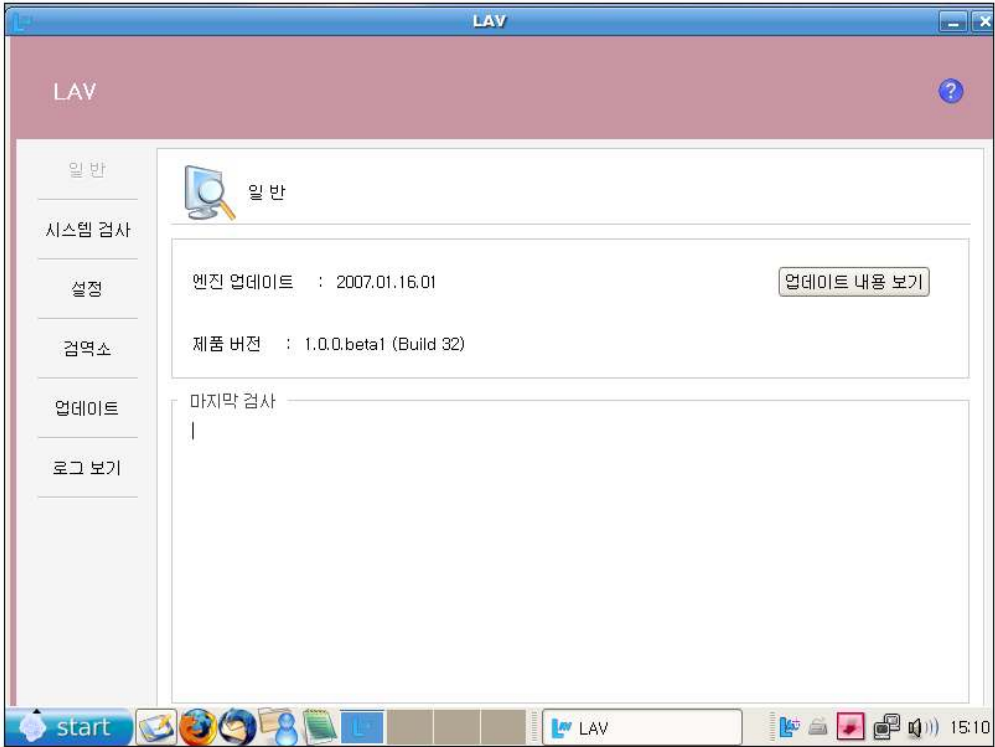
단계	항목/시험/결과	
1	시험항목	LAV 검역소
	시험절차	1. 수동 검사 후 치료한 파일들이 '검역소'에 저장되었는지 확인한다. 2. 셸 프롬프트를 이용하여 해당 경로에 바이러스 파일들이 없는지 확인한다. 3. 검역소에 저장된 파일 중 일부를 복원 기능을 통해 복원시킨다. 4. 셸 프롬프트를 이용하여 해당 경로에 파일이 이동되었는지 확인한다.
	시험결과	1. 수동 검사 후 치료한 파일들이 '검역소'에 저장되었는지 확인  <p>The screenshot shows the LAV application window. On the left is a sidebar with menu items: 일반, 시스템 검사, 설정, 검역소, 업데이트, 로그 보기. The main area is titled '검역소' and contains a table with columns: 선택, 파일, 원본 경로, 보관 날짜, 바이러스 명. Two files are listed, both from eicar.com.</p> 2. 셸 프롬프트를 이용하여 해당 경로에 바이러스 파일들이 없는지 확인 <pre data-bbox="464 1496 1453 1787">                     [root@test1 ~]# cd virus_test                     [root@test1 virus_test]# cd 1                     [root@test1 1]# ls -al                     total 8                     drwxr-xr-x 2 root root 4096 Jan 22 17:10 .                     drwxr-xr-x 4 root root 4096 Jan 22 17:10 ..                     [root@test1 test_zip]#                     </pre>

3. 검역소에 저장된 파일 중 일부를 복원 기능을 통해 복원



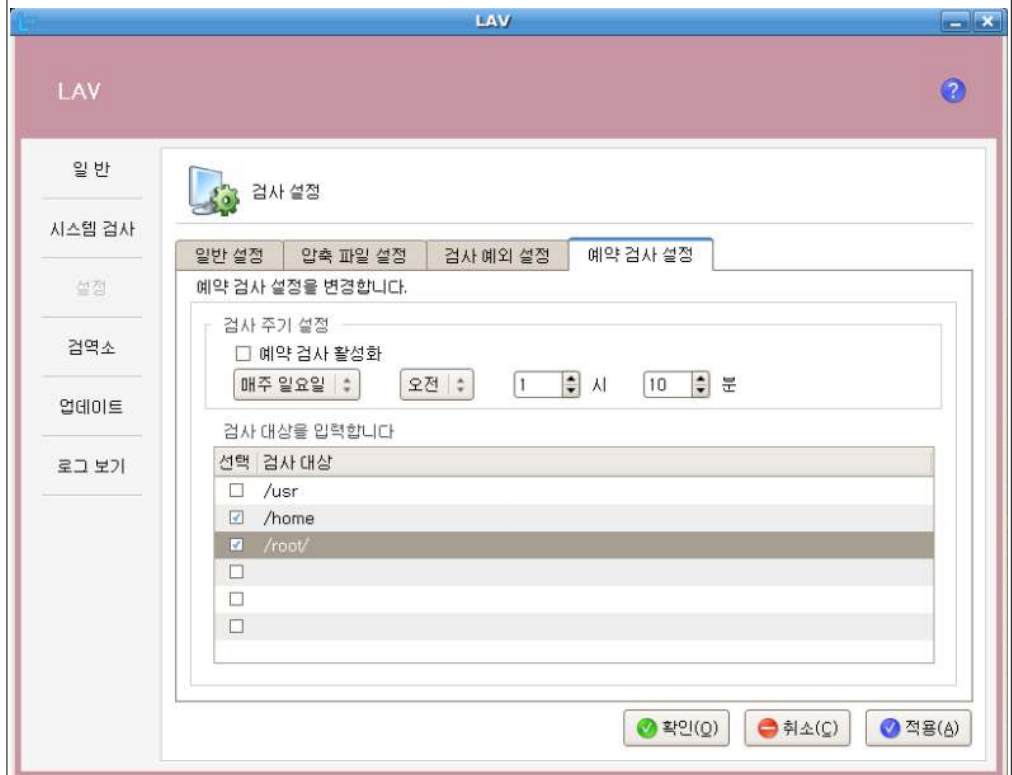


		 <p>4. 셸 프롬프트를 이용하여 해당 경로에 파일이 이동되었는지 확인</p> <pre data-bbox="464 1189 1453 1653"> [root@test1 ~]# cd virus_test [root@test1 virus_test]# cd 1 [root@test1 1]# ls -al total 8 drwxr-xr-x 2 root root 4096 Jan 22 17:10 . drwxr-xr-x 4 root root 4096 Jan 22 17:10 .. [root@test1 1]# total 12 drwxr-xr-x 2 root root 4096 Jan 22 17:32 . drwxr-xr-x 4 root root 4096 Jan 22 17:10 .. -rw-r--r-- 1 root root 68 May 24 2000 eicar.com [root@test1 1]#                     </pre>
비	고	

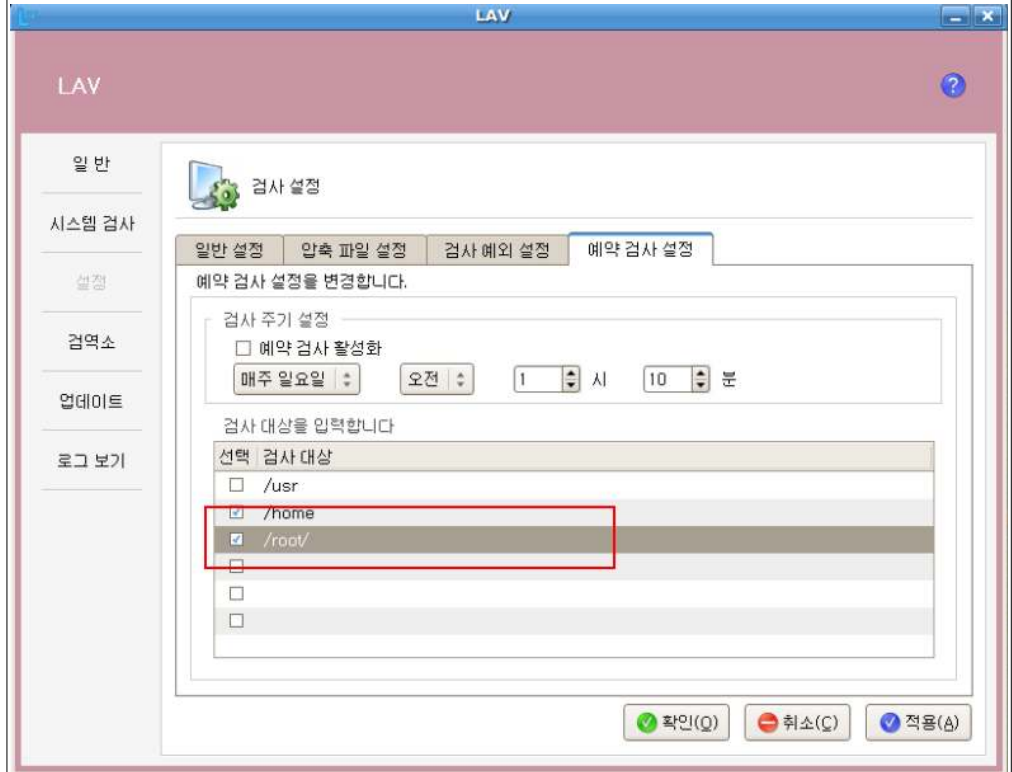
단계	항목/시험/결과	
1	시험항목	예약 검사
	시험절차	<ol style="list-style-type: none"> <li>1. X-windows로 로그인하고 LAV를 실행시킨다.</li> <li>2. [설정] 메뉴에서 '예약 검사 설정' 메뉴를 선택한다.</li> <li>3. 검사 대상 리스트에서 빈 라인을 더블클릭하고, 검사하고자 하는 디렉토리를 추가 설정한다.</li> <li>4. 검사 주기를 설정하고 '확인'을 누른다.</li> <li>5. 해당 시간에 예약 검사 기능으로 제대로 검사가 수행되는지 확인한다.</li> </ol>
	시험결과	<ol style="list-style-type: none"> <li>1. X-windows로 로그인하고 LAV 실행</li> </ol> 



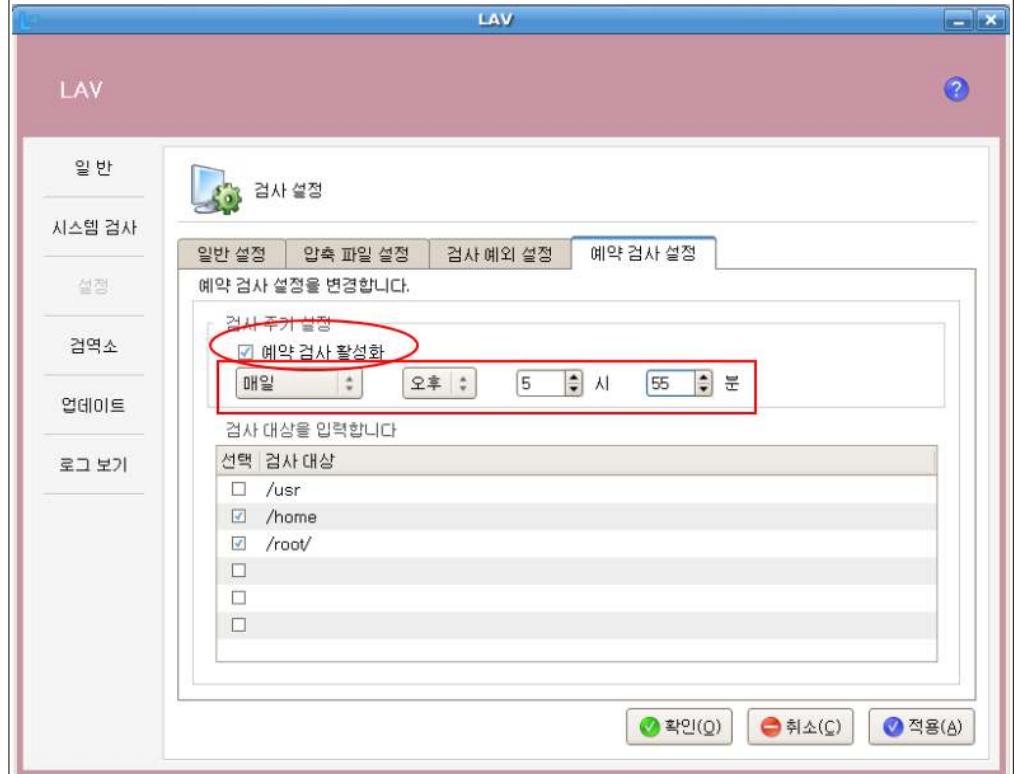
2. [설정] 메뉴에서 '예약 검사 설정' 메뉴를 선택한다.



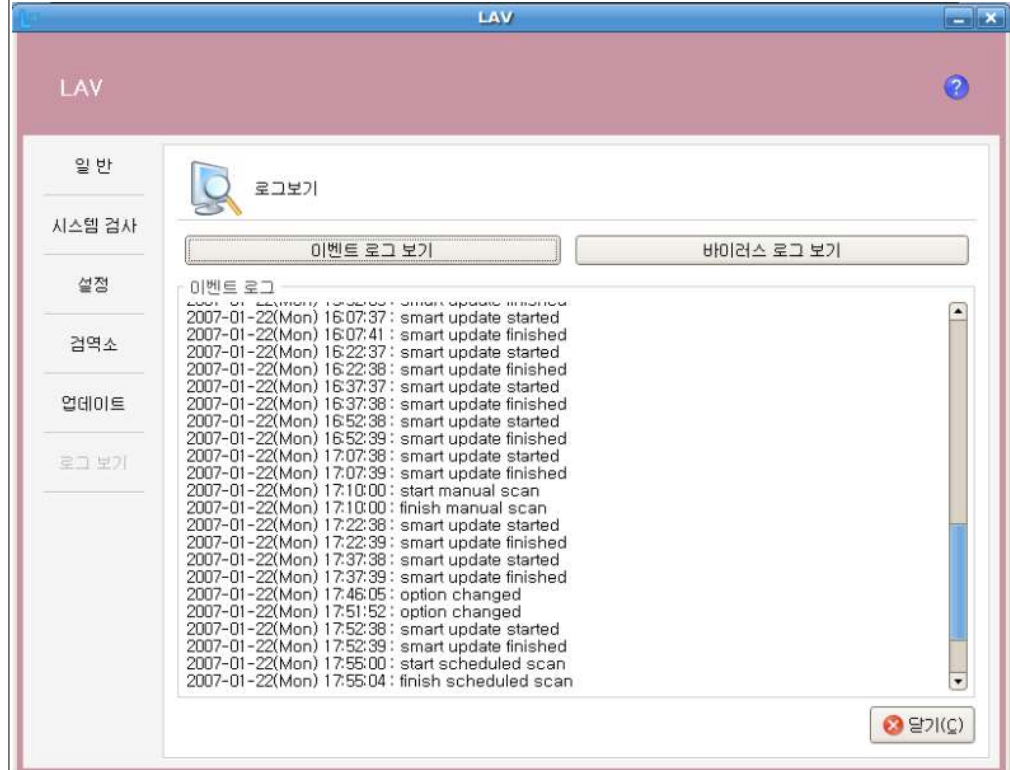
3. 검사 대상 리스트에서 빈 라인을 더블클릭하고, 검사하고자 하는 디렉토리를 추가 설정한다.



4. 검사 주기를 설정하고 '예약 검사 활성화'를 선택한 후 '적용' 및 '확인' 순으로 클릭한다.



5. [로그보기] 메뉴 중 ‘이벤트 로그 보기’ 및 ‘바이러스 로그 보기’를 선택하여, 해당 시간에 예약 검사 기능으로 검사가 수행되었는지 확인한다.



비	고	