**Cybersoft.com**


## CyberSoft White Papers

NSTL is an independent, well respected, software testing laboratory. They reviewed VFind Version 5 Release 1 in April 1996. The purpose of the test was to independently verify the functionality of the product and to identify areas where CyberSoft could improve the product. The test accomplished both of these goals, demonstrating that the product fulfilled and exceeded its requirements. The NSTL report concludes, "CyberSoft's utilities are more than antivirus utilities. ..... CyberSoft's utilities are of a unique and versatile kind in the market". Here is the exact and complete report.

---

NSTL

NATIONAL SOFTWARE TESTING LABORATORIES

---

## NSTL FINAL REPORT for CyberSoft, Inc.

### Evaluation of VFind anti-virus program

June 1996

This report was prepared by National Software Testing Laboratories, Inc. (NSTL) under contract for the CyberSoft, Inc. NSTL does not guarantee the accuracy, adequacy or completeness of the services provided in connection with this project. NSTL MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO RESULTS TO BE OBTAINED BY ANY PERSON OR ENTITY FROM USE OF THE CONTENTS OF THIS REPORT. NSTL MAKES NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF ANY PRODUCT MENTIONED IN THIS REPORT.

### I. Introduction:

CyberSoft, Inc., contracted National Software Testing Laboratories, Inc., (NSTL) to provide an independent assessment of their virus scanner program VFind and other related utilities. NSTL performed the usability and functionality of VFind and accompanying utilities. The terms and conditions for this project was subjected to NSTL CyberSoft contract, dated April 1996.

## II. Test Methodology:

NSTL and CyberSoft agreed to perform this testing in the CyberSoft Laboratories which had already installed different UNIX platforms. CyberSoft's anti-virus solution includes a set of three important UNIX utilities - VFind, Cryptographic Integrity Tool and Trojan Horse Detector.

**VFind:** This utility program is a virus scanner for a variety of UNIX systems. It can scan and identify UNIX, DOS, Amiga and Macintosh based viruses. VFind scans the contents of an entire file and checks for the signatures of viruses. NSTL observed that multiple virus signatures for DOS, Mac, Unix, and Amiga are integrated into VFind. In addition to UNIX viruses and Macro Viruses, (for example, Concept Virus which attacks Microsoft Word for Windows) VFind uses vdl files which contain virus descriptions in the form of the CyberSoft Virus Description Language (CVDL).

**Cryptographic Integrity Tool (CIT):** CIT is a utility designed using RSA's Message-Digest MD5 cryptographic technology. This utility detects the modifications, additions and deletions of any file in the UNIX system.

**Trojan Horse Detector (THD):** THD utility is used to detect duplicate file names (and their locations) in the entire system, as well as, the presence of any dangerous files. This program uses a database file called "THD.db" which contains the names of user defined dangerous/unwanted file names.

All of the above programs generate text files containing a detailed report. CyberSoft ships all of the above programs, along with example scripts, installation scripts, readme file, "Bhead" program and sample VDL libraries in a compressed format.

During the functionality test, NSTL performed the tests on two different UNIX platforms. Installation of VFind , Version 5.0, Release 1 (with CIT version 1.0) was performed on a Sun Microsystem's Solaris 2.4 operating system and on SunOS 4.1.4. CyberSoft's "example1.sh" script which uses both CIT and VFind was executed to detect viruses on the Sun 4/110 platform running the SunOS.

## III. Test Results:

**Functionality:** The "example1.sh" script, in which VFind utilizes the output of CIT, detected 4030 DOS based viruses residing in 3224 different files. This clearly indicates that VFind can detect multiple infections in a single file.

The functionality of CIT and THD were verified on the Sun Microsystems' Solaris 2.4 operating systems. CIT detected the modified and deleted files and THD reported identical files and their paths,

as well as the dangerous files requested in the "THD.db" file.

CyberSoft has already provided a work-around and has announced to provide a fix in Release 2 of VFind Version 5.0 of the following problem. When "example1.sh" was executed on the Solaris platform, it failed to execute the script normally. Error messages indicated failures to open a file, however, CyberSoft identified and fixed the problem within 24 hours. According to CyberSoft, this problem was caused only in some versions of VFind and CIT which simultaneously accessed a same scratch file called "vfind.tmp". When both these programs were executed simultaneously (from a same command line as in "examle1.sh"), both tried to open this scratch file and the unsuccessful program was terminated prematurely.

**Usability:** Unlike the off-the-shelf anti-virus programs of the DOS/Windows world, CyberSoft's VFind programs are a group of utilities that can be customized for the end-user needs. In order to minimize the complexity of retyping different commands and remembering various arguments for VFind utilities, CyberSoft ships example scripts as a package. As graphical user interfaces (GUIs) become more popular in the market, NSTL believes that the product would be more useful if it can provide a GUI. CyberSoft has informed NSTL that such interfaces will be provided in the future.

Printed user manuals are provided for CIT and VFind. The THD user manual is provided in the file called "THD.DOC". NSTL believes that it would be very helpful to users if the CIT and VFind manuals were also provided in the electronic form, as well as hard copy. The manuals focus on syntax and examples. Since CyberSoft's utilities can be used for multiple applications, NSTL believes that these alternate applications be further documented.

The usage of external CVDL files to detect viruses is very useful to the end-user to upgrade the capabilities of VFind to catch new viruses. Users will need to understand the syntax of CVDL and know the anatomy of a new virus in order to create virus scan codes in the CVDL format. Although CyberSoft does not provide free updates of VFind, it will create a CVDL file free of cost if a registered user provides the information about a new virus.

I believes that the speed VFind can be improved if it has an option to turn off the following messages:

a) to request the next file (especially when in a batch mode)

b) message stating a particular file being scanned, etc.

When performing a scan of a large UNIX system, CyberSoft recommends its users execute VFind with Unix "Cron" command so that scanning can be performed at off peak hours.

**Conclusion:** CyberSoft's utilities are more than anti-virus utilities. For example, their CIT utility can be used to verify the integrity of a transmitted file. The capability to automatically transmit a report file is very useful to remotely monitor the security of systems. Its THD can be used to eliminate unwanted programs (for example, illegal copies of programs, out-dated versions, etc.) on the systems. NSTL believes that customers would benefit if CyberSoft mentions examples of other applications of CyberSoft's utilities.

The number (which is increasing) of known UNIX viruses in the market is significantly less than the number of known DOS and Macintosh viruses. In addition to catching all these UNIX viruses, CyberSoft's one program provides complete protection against thousands of other platform viruses. The capability of CyberSoft's utilities to work on more than twenty platforms and display messages in many languages (customized versions) is a definite plus. This is very helpful for heterogeneous networks which are becoming very common. VFind's capability to detect the latest generation of DOS based viruses (Stealth, Self Mutating, Polymorphic, etc.) could not be tested due to the unavailability of such viruses.

CyberSoft's utilities are of a unique and versatile kind in the market.







508 Compliance TestPros TESTED

This site certified 508 Compliant