



CyberSoft White Papers

Special Attributes of the VFind Tool Kit

Peter V. Radatti
CyberSoft, Inc.

Copyright © May 1997 by Peter V. Radatti. All Rights Reserved.

The VFind Tool Kit is not a specific purpose product but rather a set of tools that can be used to solve multiple problems. This is not surprising because just as the name implies, the product is actually a tool kit. Just as a screwdriver can be used to repair an automobile, install a light switch or pry open a paint can, the tools in the VFind tool kit can be used for a myriad of purposes, most of which were not originally thought of by the designers.

Some of the purposes customers have used the VFind Tool Kit for are;

1) Antivirus

The product was actually designed as an antivirus product for UNIX so this is not a surprise. Since VFind is heterogeneous, many customers have been using VFind to scan their DOS and Macintosh emulators on their UNIX systems. In addition, since many UNIX systems tend to be used as file servers, it is common for VFind to be used to scan exported file systems for PCs and other systems. Finally, a few customers have interfaced VFind to their document management systems such as Documentum.

2) Email Legal Issues (Confidential, SEC, Certified)

When using email for EDI or contractual information interchange, the CIT program can be used to create a unique and provable relationship between email, each other and the date and time. In effect, this allows you to create "Certified Email".

3) Help Desk Overhead (Baseline Control)

One of the biggest problems with customer support is overhead costs associated with a help desk. These costs generally have nowhere to go but up. Our studies have indicated that the bulk of a customer service call is spent doing diagnosis. Generally the end user does not know why their system is not working but they are sure that they didn't change anything. For a complex operating system such as UNIX, Windows NT or Windows 95 this can take up to 2 hours to resolve. Using CIT, a system can be baselined when it is installed and updated. At anytime in the future if the system fails, the Help Desk can run CIT again and it will reveal every file which has been added, deleted or modified. This can reduce the time for diagnoses to about 15 minutes.

4) Key Word Searches (Classified, lost documents)

Many companies use keywords in documents and programs to protect propriety information, (COMPANY CONFIDENTIAL). Standard key word searching tools are not a reliable way of searching for keywords because the word processor may represent them internally in a way that is not expected. In addition, Microsoft Word can encrypt parts of documents such as macros. The VFind CVDL system provides a way to solve this problem. Using case insensitivity and proximity scanning key words and phrases can be reliably searched for even inside binary programs. Using the next release of UAD allows CVDL to automatically crack Word encrypted document segments for scanning. These tools can also be used to search for lost documents or to find all documents on a network dealing with a certain subject such as a new product or project.

5) Hacker/Disgruntled Employee Attacks

Not only does VFind have known hacker attacks captured in its internal database but it is impossible to escape the CIT cryptographic integrity system. Using VFind with CIT insures that all hacker or disgruntled employee attacks on critical system files are revealed.

6) Archival Integrity

Magnetic archival copies of data are subject to change caused by degradation of the signal, random radiation and accidental overwrite. Using CIT to create a cryptographic integrity signature (hash code) you can always be sure that what you are reading and using today is what was written yesterday. This resolves a major problem for tape librarians.

7) Certified File Transfers

When the Internet is used to transfer files, there is always a good possibility that the byte stream is modified by undetected error or by intentional tampering. Using CIT to create a hash code for the file, the data can be transferred and if the hash code at the other end matches the file it is mathematically proven to be the same.

8) Internet File Cracking (File cracking, Data Warehouse)

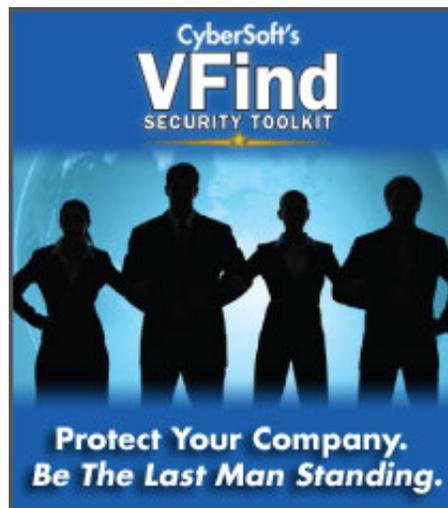
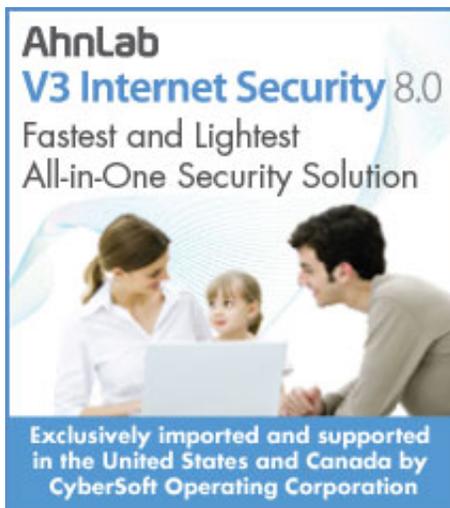
When downloading files from the Internet, the data may not be in a format that is usable. For example, you may be using a Windows 95 system but the data was received as a uuencoded, UNIX compressed tar file. This would cause you to have to find a UNIX system, transfer the data, manually uuencode, uncompress and tar extract it then ftp all of the data back to your system where it is needed. This problem is resolved by UAD. The command "UAD -f filename" will crack most files down to their component level. This is also useful in data warehousing operations. Not only does UAD insure that all received data is broken down to a consistent level but it identifies every file as to type by its content.

9) Java Attacks

Later this year VFind will be the first antivirus product to detect Java attacks. There are already Java viruses, in addition to browser attacks. We expect to deliver the first Java detection in June 1997.

10) One Product All Systems

One of the best benefits of VFind is that one package runs on all 32 bit systems. We support about 25 different versions of UNIX, Linux and Microsoft NT / Windows-95.



[Home](#) | [Products](#) | [Support](#) | [Purchase](#) | [Contact](#) | [News](#) | [About](#)

© Copyright 2010 CyberSoft, Inc. All rights reserved.



This site certified 508 Compliant