

PACKAGE ID - 000295I600000 W&S 3.0.1

KWIC TITLE - Wisdom and Sense

AUTHORS - Redle, K.
Los Alamos National Lab, NM (United States)

LIMITATION CODE -COPY **AUDIENCE CODE** - LIM

COMPLETION DATE - 11/01/1991 **PUBLICATION DATE** - 03/03/1992

DESCRIPTION - W&S is a system that evolved to address a specific albeit very broad, class of problems. Initial work focused on detecting clerical errors in materials accounting data. From this start, W&S was extended to identify all types of rare materials accounting transactions. Next, W&S was rebuilt and enhanced to deal with computer security audit trails. In this problem area, W&S was configured to look for evidence of computer misuse. Finally, W&S was enhanced and extended to improve its generality and better accommodate process control data and network security data. W&S can simultaneously gather data from multiple, networked sources; filter (select and transform) raw transaction data; compute data aggregations and other derived quantities; automatically detect normal behavior patterns; accept and apply expert knowledge of behavior; and find anomalies (non-conforming behavior).

PACKAGE CONTENTS - Software Abstract; Installation Instructions (4 pages);

SOURCE CODE INCLUDED? - No

MEDIA QUANTITY - 1 CD Rom

METHOD OF SOLUTION - W&S is a collection of capabilities for creating models of behavior, predicting behavior and detecting non-confirming behavior. These capabilities use data records called transactions to build models. W&S is then able to predict the contents of a transaction from partial data and to detect non-confirming transactions.

COMPUTER - IBM RS 6000

OPERATING SYSTEMS - UNIX

PROGRAMMING LANGUAGES - C

SOFTWARE LIMITATIONS - At this stage of it life-cycle, W&S is an evolving research tool still in it's proof-of-concept stage. It does not have a user interface that is appropriate for mass distribution, nor it is fully debugged. Perhaps most trying for the W&S user is the difficulty in configuring W&S.

SOURCE CODE AVAILABLE (Y/N) - N

PACKAGE ID - 000295I600000 W&S 3.0.1

UNIQUE FEATURES - The W&S interface is functional but relatively unadorned. The interface permits experienced W&S users to configure the system to process practically any transaction format with little preprocessing for formatting. In essence, W&S can be configured to a transaction in its native format. Internally, the native data is converted to W&S standard data representations. Once the native data is in this internal format, W&S applies a powerful set of capabilities to further transform and analyze the data.

OTHER PROG/OPER SYS INFO - It is not expected that persons interested in the concept attempt to build an executable from the sources provided. Therefore, neither a MAKE file nor machine-dependent TERMINFO files have been provided. LANL has not assigned staff necessary to provide support for W&S because it is being used solely as a research tool. Nor is additional documentation available.

ABSTRACT STATUS - Released AS-IS 7/26/95.

SUBJECT CLASS CODE - P

KEYWORDS -

COMPUTER PROGRAM DOCUMENTATION
W CODES
EXPERT SYSTEMS
KNOWLEDGE BASE
BEHAVIOR
LEARNING

EDB SUBJECT CATEGORIES -
990200

SPONSOR - DOE/DP

PACKAGE TYPE - AS - IS