US007210041B1

(12) **United States Patent**
Gryaznov et al.

(10) **Patent No.:** **US 7,210,041 B1**
(45) **Date of Patent:** **Apr. 24, 2007**

(54) **SYSTEM AND METHOD FOR IDENTIFYING A MACRO VIRUS FAMILY USING A MACRO VIRUS DEFINITIONS DATABASE**

(75) Inventors: **Dmitry O. Gryaznov**, Portland, OR (US); **Viatcheslav Peternev**, Bucks (GB); **Igor Muttik**, Herts (GB)

(73) Assignee: **McAfee, Inc.**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 738 days.

(21) Appl. No.: **09/846,103**

(22) Filed: **Apr. 30, 2001**

(51) **Int. Cl.**
G06F 11/00 (2006.01)
G06F 17/30 (2006.01)

(52) **U.S. Cl.** **713/188**; 714/38; 395/182; 395/183

(58) **Field of Classification Search** 713/200, 713/201; 395/183, 575
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,414,833	A	*	5/1995	Hershey et al.	713/201
5,448,668	A	*	9/1995	Perelson et al.	714/21
5,452,442	A	*	9/1995	Kephart	714/38
5,485,575	A	*	1/1996	Chess et al.	714/38
5,951,698	A	*	9/1999	Chen et al.	714/38
5,960,170	A	*	9/1999	Chen et al.	714/38
6,016,546	A	*	1/2000	Kephart et al.	713/200
6,067,410	A	*	5/2000	Nachenberg	703/28
6,577,920	B1	*	6/2003	Hypponen et al.	700/200
6,647,400	B1	*	11/2003	Moran	707/205
6,721,721	B1	*	4/2004	Bates et al.	707/1
6,748,534	B1	*	6/2004	Gryaznov et al.	713/188
6,892,303	B2	*	5/2005	Le Pennec et al.	713/188
6,963,978	B1	*	11/2005	Muttik et al.	713/188
7,093,135	B1	*	8/2006	Radatti et al.	713/188

OTHER PUBLICATIONS

Office Action Summary from U.S. Appl. No. 09/579,810 which was mailed on Feb. 25, 2005.

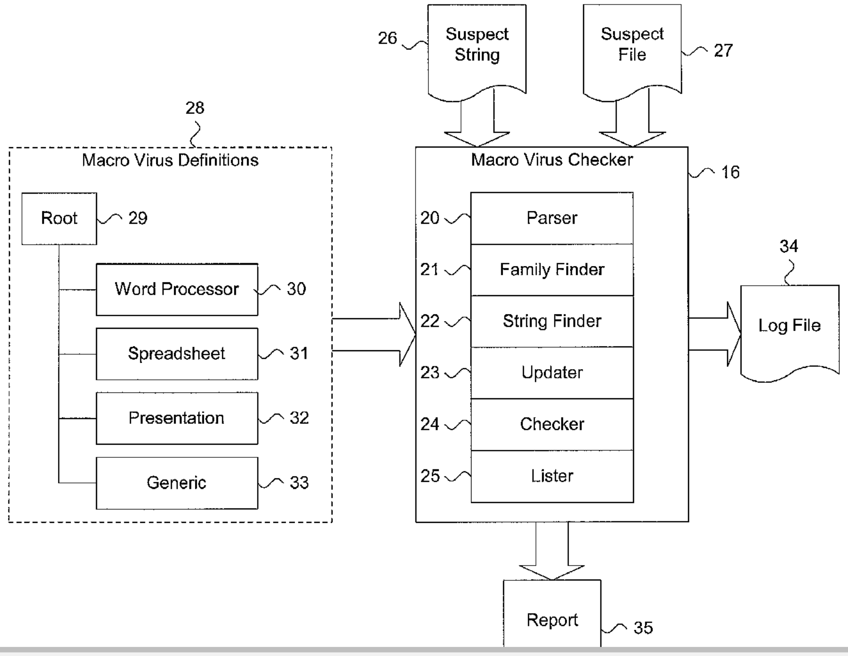
* cited by examiner

Primary Examiner—Nasser Moazzami
Assistant Examiner—Carl Colin
(74) *Attorney, Agent, or Firm*—Zilka-Kotab, PC; Christopher J. Hamaty

(57) **ABSTRACT**

A macro virus definitions database is maintained and includes a set of indices and associated macro virus definition data files. One or more of the macro virus definition data files are referenced by the associated index. Each macro virus definition data file defines macro virus attributes for known macro viruses. The sets of the indices and the macro virus definition data files are organized according to macro virus families. One or more strings stored in a suspect file are compared to the macro virus attributes defined in the one or more macro virus definition data files for each macro virus family in the macro virus definitions database. The macro virus family to which the suspect file belongs is determined from the indices for each of the macro virus definition data files at least partially containing the suspect file.

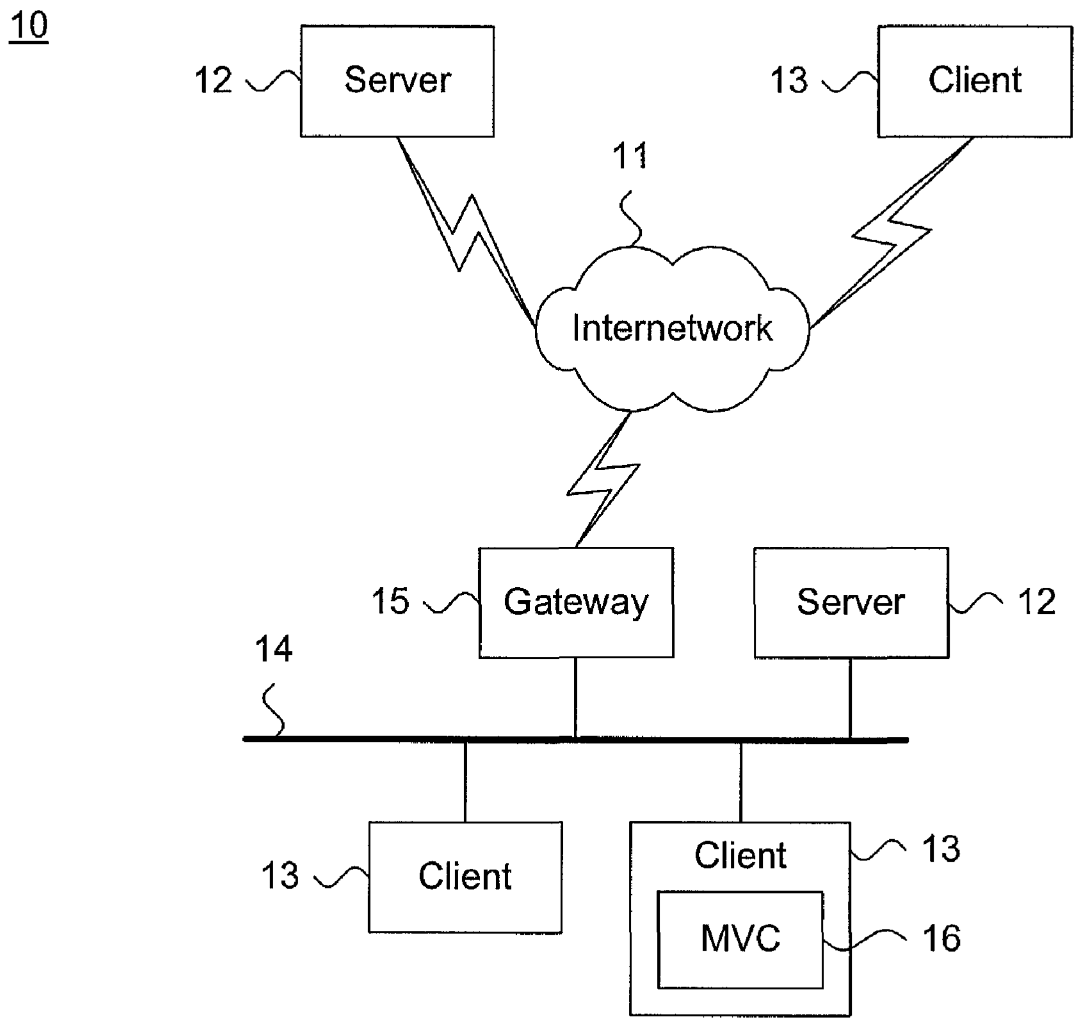
16 Claims, 21 Drawing Sheets



DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

DOCKET
ALARM
Find authenticated court documents without watermarks at docketalarm.com.

Figure 1.



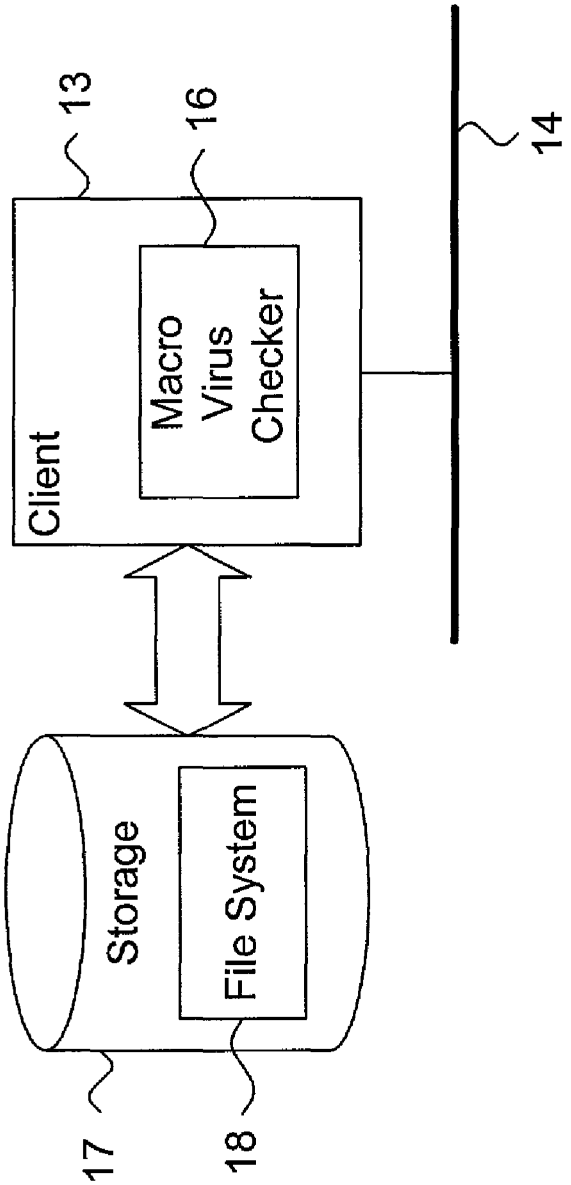


Figure 2.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

Figure 3.

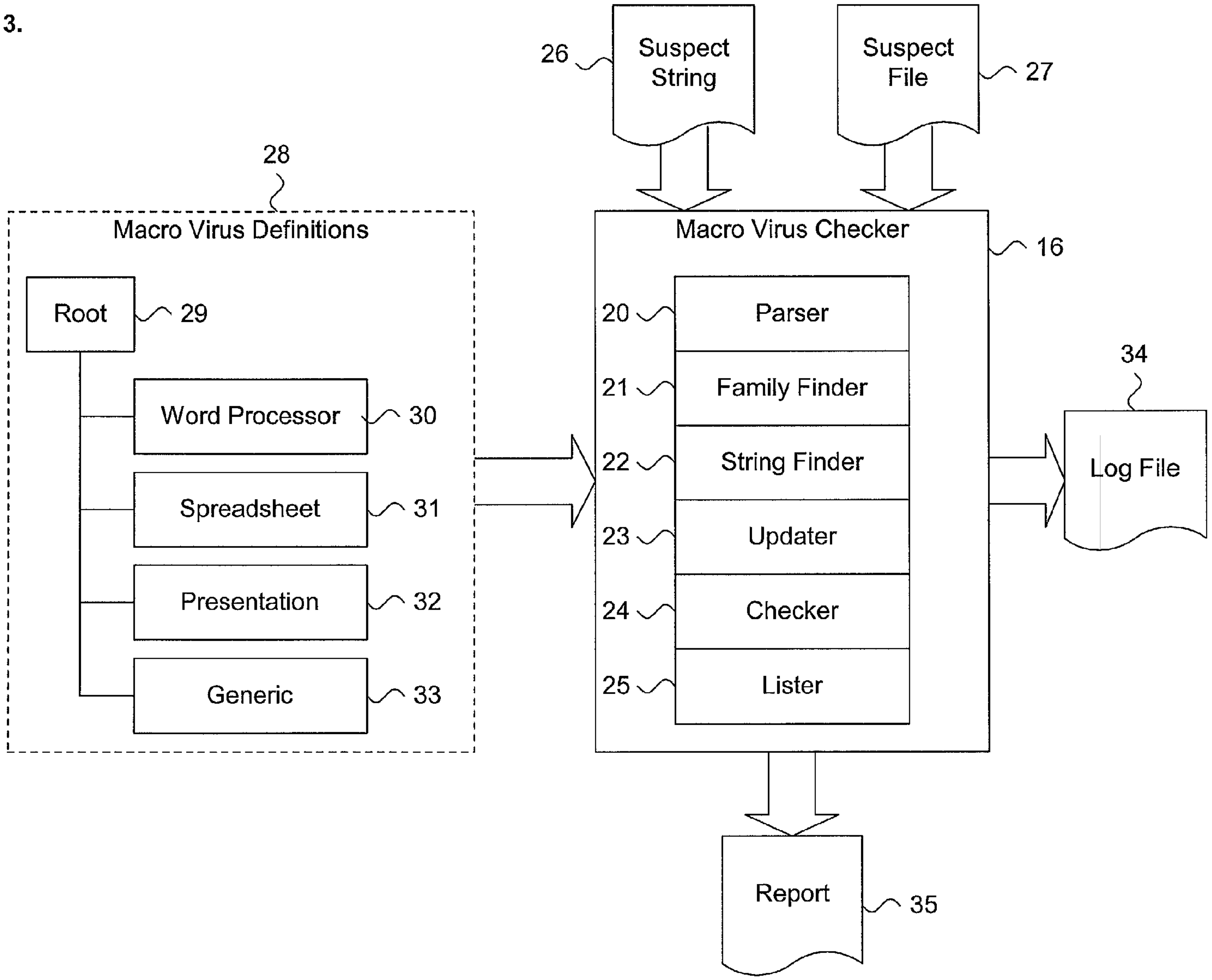
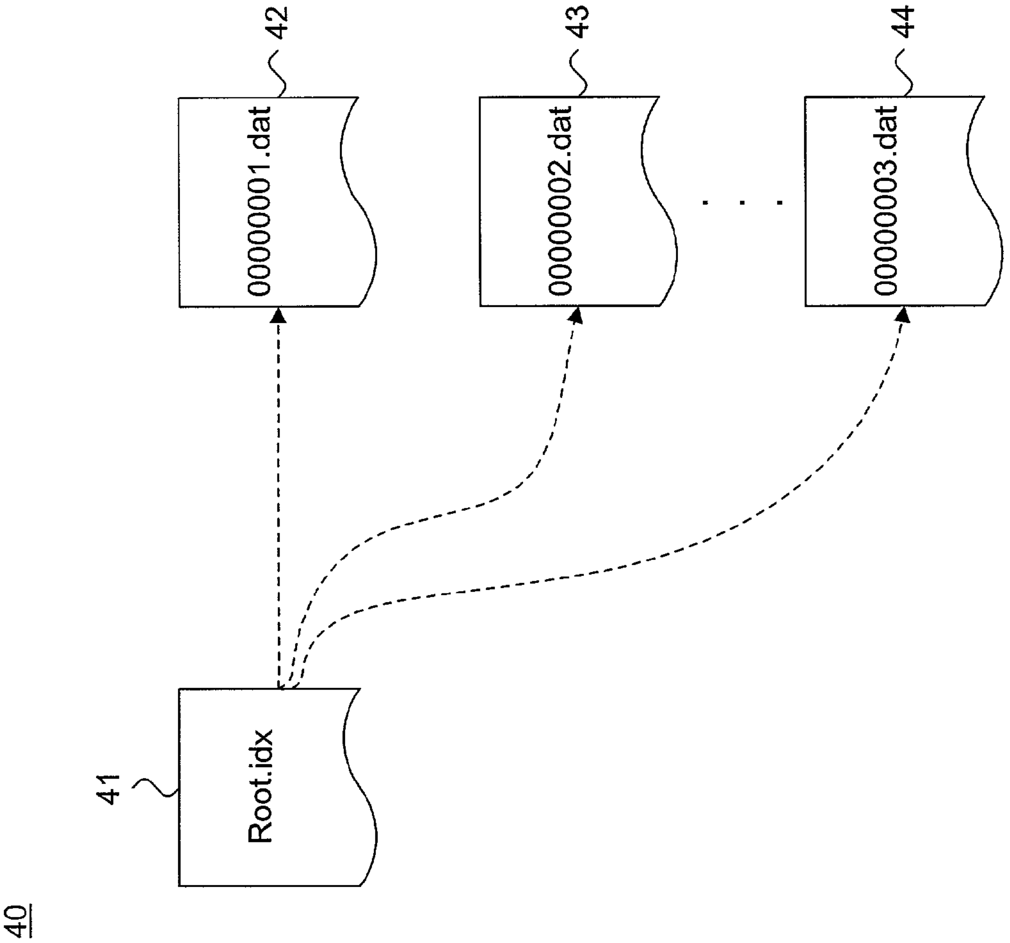


Figure 4.



DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.