



US006651099B1

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

(10) **Patent No.: US 6,651,099 B1**  
(45) **Date of Patent: Nov. 18, 2003**

(54) **METHOD AND APPARATUS FOR MONITORING TRAFFIC IN A NETWORK**

5,375,070 A 12/1994 Hershey et al. .... 364/550  
5,394,394 A 2/1995 Crowther et al. .... 370/60

(75) Inventors: **Russell S. Dietz**, San Jose, CA (US);  
**Joseph R. Maixner**, Aptos, CA (US);  
**Andrew A. Koppenhaver**, Littleton, CO (US);  
**William H. Bares**, Germantown, TN (US);  
**Haig A. Sarkissian**, San Antonio, TX (US);  
**James F. Torgerson**, Andover, MN (US)

(List continued on next page.)

**OTHER PUBLICATIONS**

“Technical Note: the Narus System,” Downloaded Apr. 29, 1999 from www.narus.com, Narus Corporation, Redwood City California.

*Primary Examiner*—Moustafa M. Meky

(74) *Attorney, Agent, or Firm*—Dov Rosenfeld; Inventek

(73) Assignee: **Hi/fn, Inc.**, Los Gatos, CA (US)

(57) **ABSTRACT**

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 589 days.

A monitor for and a method of examining packets passing through a connection point on a computer network. Each packets conforms to one or more protocols. The method includes receiving a packet from a packet acquisition device and performing one or more parsing/extraction operations on the packet to create a parser record comprising a function of selected portions of the packet. The parsing/extraction operations depend on one or more of the protocols to which the packet conforms. The method further includes looking up a flow-entry database containing flow-entries for previously encountered conversational flows. The lookup uses the selected packet portions and determining if the packet is of an existing flow. If the packet is of an existing flow, the method classifies the packet as belonging to the found existing flow, and if the packet is of a new flow, the method stores a new flow-entry for the new flow in the flow-entry database, including identifying information for future packets to be identified with the new flow-entry. For the packet of an existing flow, the method updates the flow-entry of the existing flow. Such updating may include storing one or more statistical measures. Any stage of a flow, state is maintained, and the method performs any state processing for an identified state to further the process of identifying the flow. The method thus examines each and every packet passing through the connection point in real time until the application program associated with the conversational flow is determined.

(21) Appl. No.: **09/608,237**

(22) Filed: **Jun. 30, 2000**

**Related U.S. Application Data**

(60) Provisional application No. 60/141,903, filed on Jun. 30, 1999.

(51) **Int. Cl.**<sup>7</sup> ..... **G06F 13/00**

(52) **U.S. Cl.** ..... **709/224; 370/389**

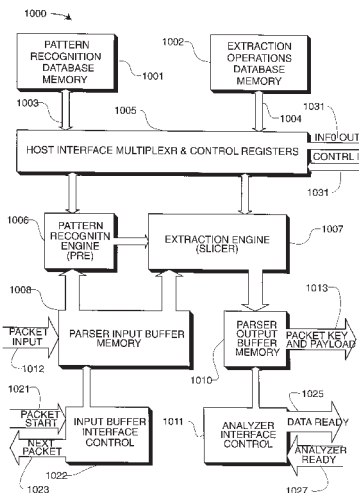
(58) **Field of Search** ..... 709/200, 201,  
709/220, 223, 224, 231, 232, 236, 238,  
239, 240, 246; 370/389, 392, 395.32

(56) **References Cited**

**U.S. PATENT DOCUMENTS**

4,736,320 A	4/1988	Bristol	364/300
4,891,639 A	1/1990	Nakamura	340/825.5
5,101,402 A	3/1992	Chui et al.	370/17
5,247,517 A	9/1993	Ross et al.	370/85.5
5,247,693 A	9/1993	Bristol	395/800
5,249,292 A	9/1993	Chiappa	395/650
5,315,580 A	5/1994	Phaal	370/13
5,339,268 A	8/1994	Machida	365/49
5,351,243 A	9/1994	Kalkunte et al.	370/92
5,365,514 A	11/1994	Hershey et al.	370/17

**10 Claims, 18 Drawing Sheets**



U.S. PATENT DOCUMENTS

5,414,650 A	5/1995	Hekhuis .....	364/715.02	5,802,054 A	9/1998	Bellenger .....	370/351
5,414,704 A	5/1995	Spinney .....	370/60	5,805,808 A	9/1998	Hansani et al. ....	395/200.2
5,430,709 A	7/1995	Galloway .....	370/13	5,812,529 A	9/1998	Czarnik et al. ....	370/245
5,432,776 A	7/1995	Harper .....	370/17	5,819,028 A	10/1998	Manghirmalani	
5,493,689 A	2/1996	Waclawsky et al. ....	395/821			et al. ....	395/185.1
5,500,855 A	3/1996	Hershey et al. ....	370/17	5,825,774 A	10/1998	Ready et al. ....	370/401
5,511,213 A	4/1996	Correa .....	395/800	5,835,726 A	11/1998	Shwed et al. ....	395/200.59
5,511,215 A	4/1996	Terasaka et al. ....	395/800	5,838,919 A	11/1998	Schwaller et al. ....	395/200.54
5,568,471 A	10/1996	Hershey et al. ....	370/17	5,841,895 A	11/1998	Huffman .....	382/155
5,574,875 A	11/1996	Stansfield et al. ....	395/403	5,850,386 A	12/1998	Anderson et al. ....	370/241
5,586,266 A	12/1996	Hershey et al. ....	395/200.11	5,850,388 A	12/1998	Anderson et al. ....	370/252
5,606,668 A	2/1997	Shwed .....	395/200.11	5,862,335 A	1/1999	Welch, Jr. et al. ....	395/200.54
5,608,662 A	3/1997	Large et al. ....	364/724.01	5,878,420 A	3/1999	de la Salle .....	707/10
5,634,009 A	5/1997	Iddon et al. ....	395/200.11	5,893,155 A	4/1999	Cheriton .....	711/144
5,651,002 A	7/1997	Van Seters et al. ....	370/392	5,903,754 A	5/1999	Pearson .....	395/680
5,684,954 A	11/1997	Kaiserswerth et al. ...	395/200.2	5,917,821 A	6/1999	Gobuyan et al. ....	370/392
5,703,877 A	12/1997	Nuber et al. ....	370/395	6,014,380 A	1/2000	Hendel et al. ....	370/392
5,732,213 A	3/1998	Gessel et al. ....	395/200.11	6,118,760 A	* 9/2000	Zaumen et al. ....	370/229
5,740,355 A	4/1998	Watanabe et al. ....	395/183.21	6,243,667 B1	* 6/2001	Kerr et al. ....	703/27
5,761,424 A	6/1998	Adams et al. ....	395/200.47	6,452,915 B1	* 9/2002	Jorgensen .....	370/338
5,764,638 A	6/1998	Ketchum .....	370/401	6,453,360 B1	* 9/2002	Muller et al. ....	709/250
5,781,735 A	7/1998	Southard .....	395/200.54	6,466,985 B1	* 10/2002	Goyal et al. ....	709/238
5,784,298 A	7/1998	Hershey et al. ....	364/557	6,483,804 B1	* 11/2002	Muller et al. ....	370/230
5,787,253 A	7/1998	McCreery et al. ....	395/200.61	6,570,875 B1	* 5/2003	Hegde .....	370/389

\* cited by examiner

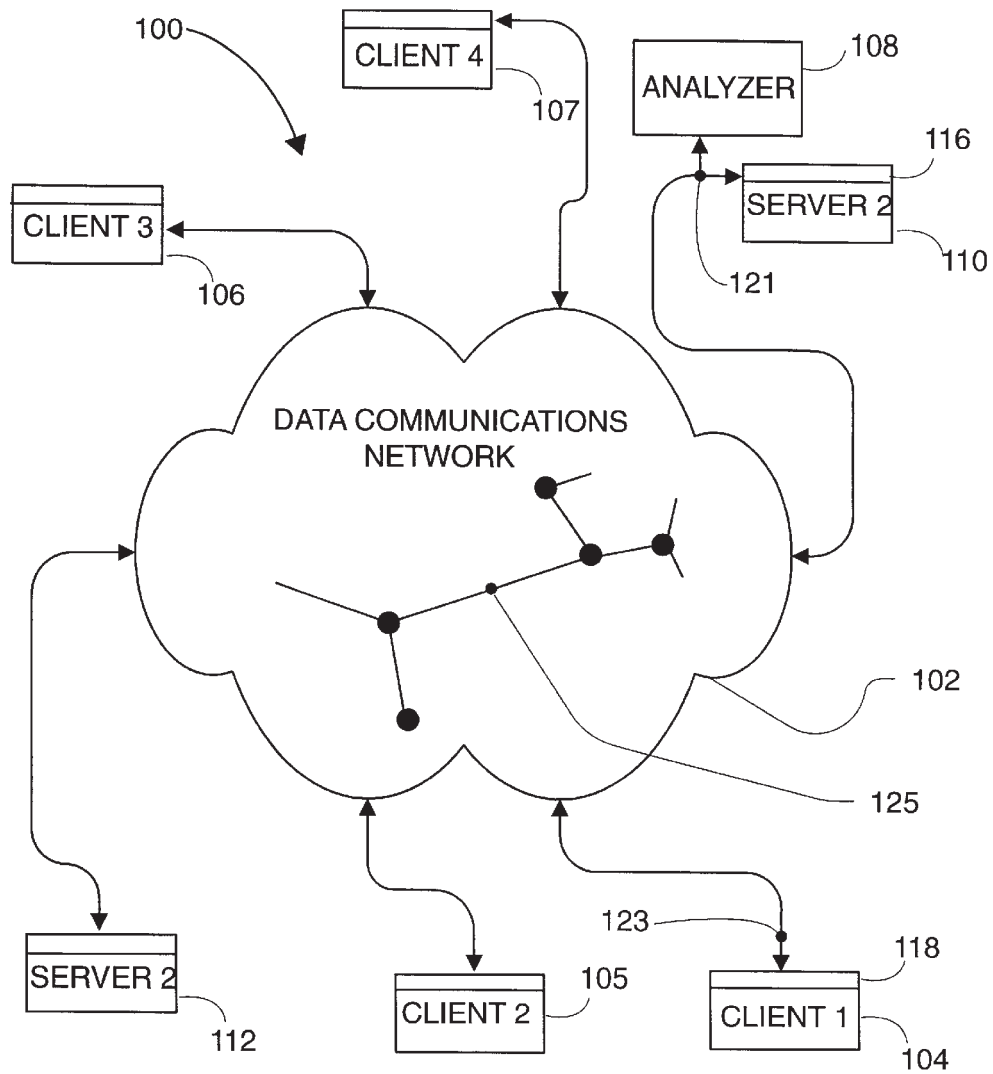
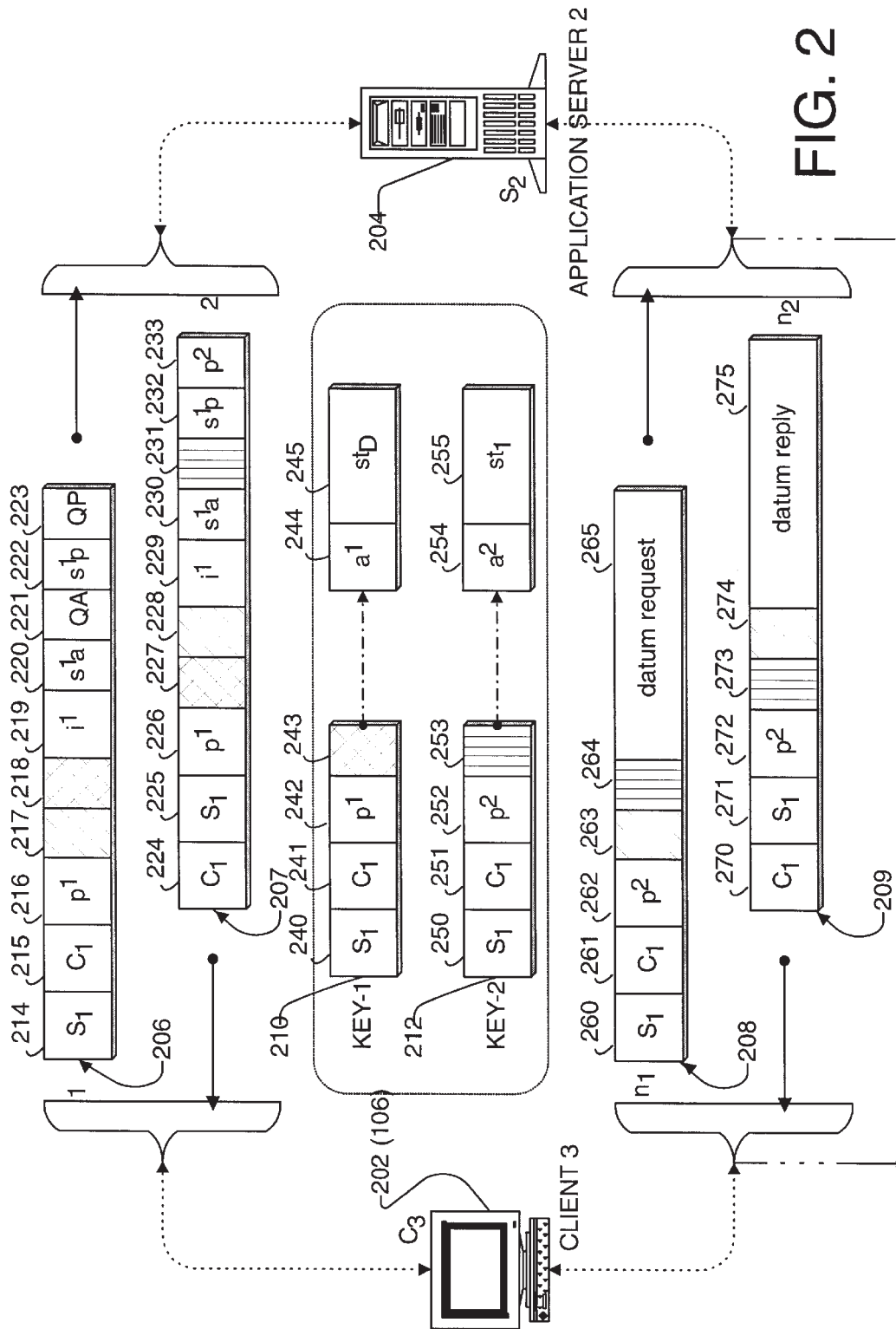


FIG. 1



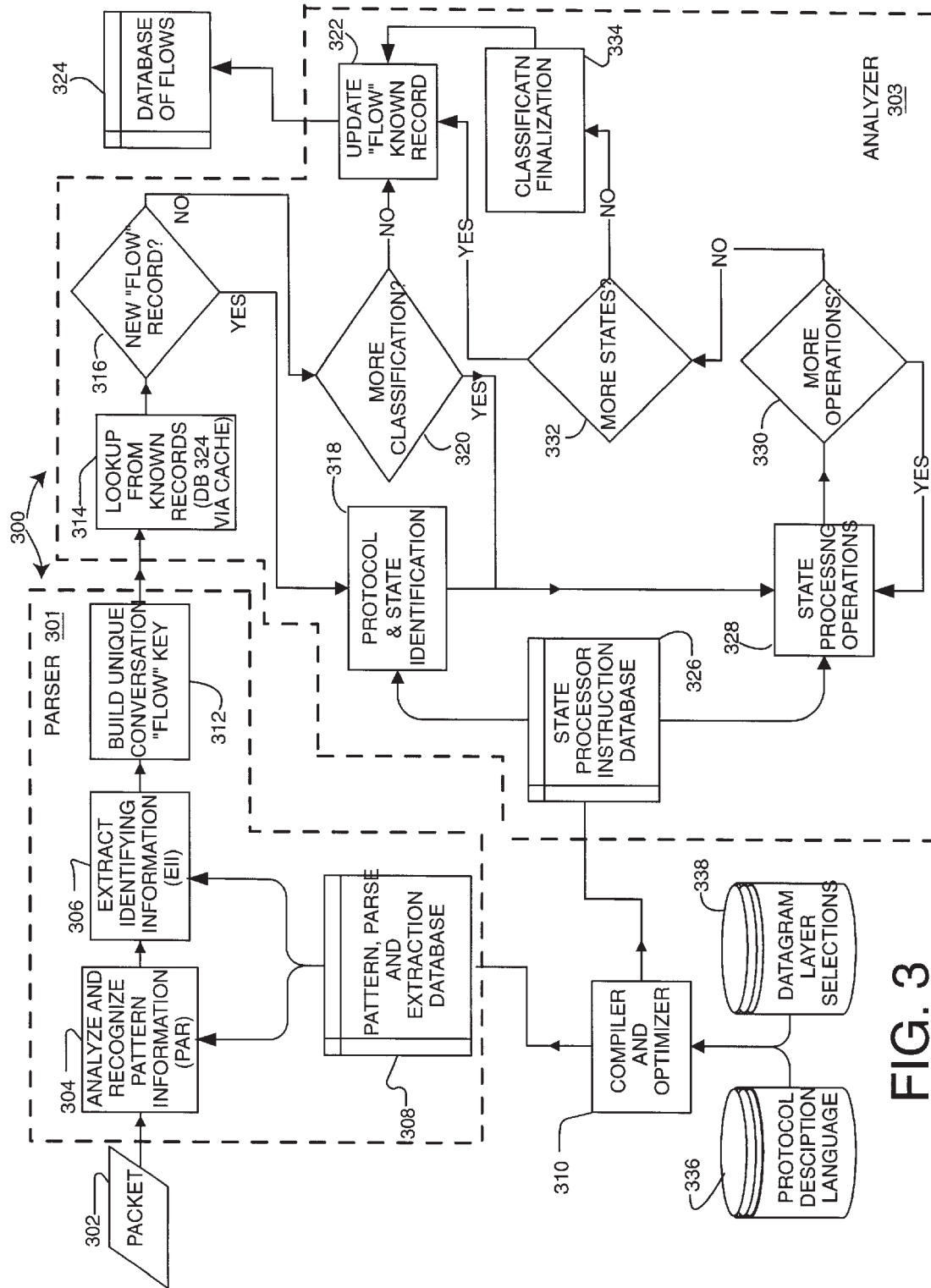


FIG. 3

# 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.