(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 October 2007 (18.10.2007)

PCT

(10) International Publication Number
WO 2007/118096 A2

(51) International Patent Classification:
G06F 11/00 (2006.01)

(21) International Application Number:
PCT/US2007/065886

(22) International Filing Date: 3 April 2007 (03.04.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/398,863 5 April 2006 (05.04.2006) US

(71) Applicant *(for all designated States except US)*: **ARCSIGHT, INC.** [US/US]; 5 Results Way, Cupertino, CA 95014 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **AGUILAR-MACIAS, Hector** [MX/US]; P.O. Box 2913, Sunnyvale, CA 94087 (US). **MANTRY, Girish** [US/US]; 3203 Myles Court, #1, San Jose, CA 95117 (US).

(74) Agents: **TRUESDALE, Sabra-Anne** et al.; Fenwick & West LLP, Silicon Valley Center, 801 California Street, Mountain View, CA 94041 (US).

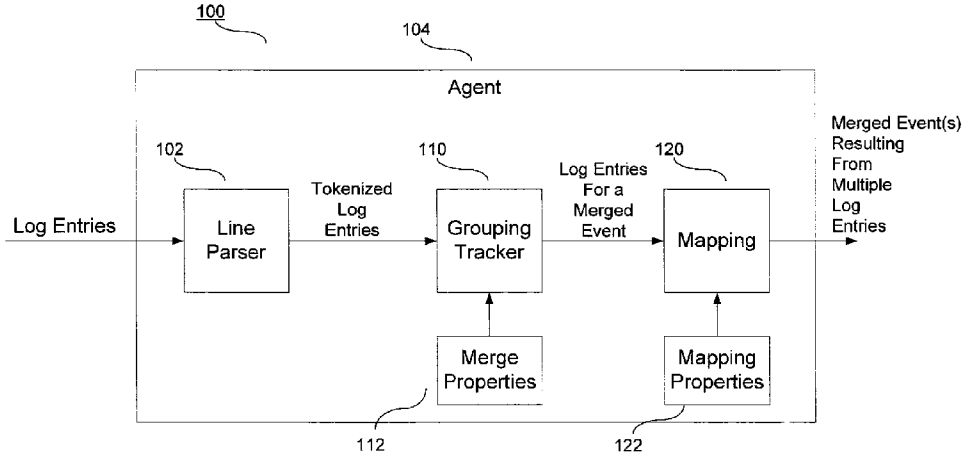
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** MERGING MULTI-LINE LOG ENTRIES



(57) **Abstract:** A system and method for building merged events from log entries received from multiple devices. Multiple log events generally contribute to a single merged event. In the described embodiment, the mapping module receives log entries associated with specific merged events and maps them to fields in the merged event data structure in accordance with mapping properties. The described embodiments of the invention use regular expressions in the merge properties to describe values that are searched for in the received log entries. A described embodiment of the present invention gives the mapping module access to the event under construction. A new conditional operator, _oneOf, is introduced that selects the first token that is bound to a value out of a list of tokens.

WO 2007/118096 A2