



- (51) **International Patent Classification:**
H04L 12/26 (2006.01) *G06F 21/50* (2013.01)
- (21) **International Application Number:**
PCT/US2014/029426
- (22) **International Filing Date:**
14 March 2014 (14.03.2014)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
61/784,931 14 March 2013 (14.03.2013) US
- (71) **Applicant: GENERAL DYNAMICS ADVANCED INFORMATION SYSTEMS, INC.** [US/US]; 12450 Fair Lakes Circle, Fairfax, Virginia 22033 (US).
- (72) **Inventors; and**
- (71) **Applicants : SAVCHUK, Gene** [US/US]; 4416 East West Hwy #310, Bethesda, Maryland 20814 (US).
ARORA, Anubhav [US/US]; 4416 East West Hwy #310, Bethesda, Maryland 20814 (US).
- (74) **Agent: BERRY, Tom;** Ingrassia, Fisher & Lorenz, P.C., 7010 E. Cochise Rd., Scottsdale, Arizona 85253 (US).
- (81) **Designated States** (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

[Continued on next page]

(54) **Title:** SYSTEM AND METHOD FOR EXTRACTING AND PRESERVING METADATA FOR ANALYZING NETWORK COMMUNICATIONS

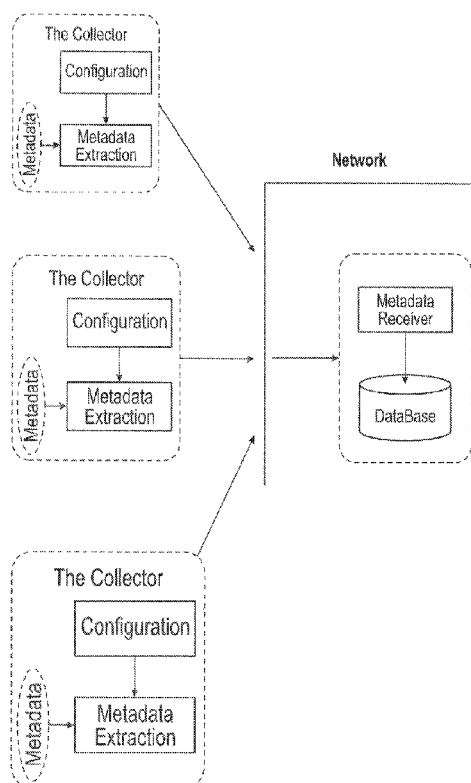


FIG. 6

(57) **Abstract:** Systems and methods are provided for advanced persistent threat detection on a network. The method includes capturing data packets from a network and performing layered session decoding on the captured packets. Metadata is extracted from the decoded packets and is stored for analysis. Analysis of the metadata is used to detect advanced persistent threats on the network. The system includes a network and a processor coupled to the network. The processor is configured to capture data packets from the network and perform layered session decoding on the captured packets. Metadata is extracted by the processor and stored in a memory coupled to the processor. The metadata may then be analyzed to detect advanced persistent threats on the network.



TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, —
KM, ML, MR, NE, SN, TD, TG).

*before the expiration of the time limit for amending the
claims and to be republished in the event of receipt of
amendments (Rule 48.2(h))*

Published:

— *with international search report (Art. 21(3))*