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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 September 2002 (12.09.2002)

PCT

(10) International Publication Number
WO 02/071192 A3

(51) International Patent Classification[7]: G06F 11/60

(21) International Application Number: PCT/US02/06622

(22) International Filing Date: 5 March 2002 (05.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/800,378 5 March 2001 (05.03.2001) US

(71) Applicant: **SECURIFY, INC.** [US/US]; 1157 San Antonio Road, Mountain View, CA 94043 (US).

(72) Inventor: **DE LA GARZA, Joel**; 3553 Alma Apt., 3, Palo Alto, CA 94304 (US).

(74) Agents: **GLENN, Michael** et al.; Glenn Patent Group, 3475 Edison Way, Ste. L., Menlo Park, CA 94025 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

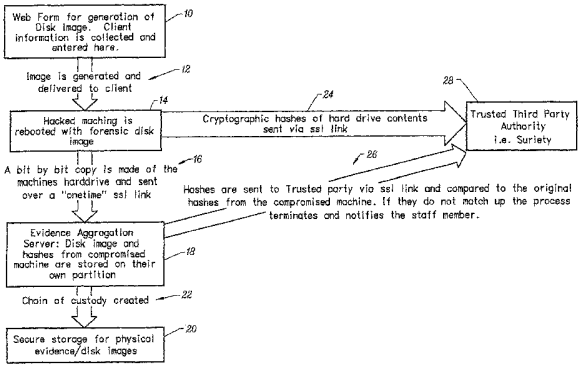
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
20 February 2003

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: REMOTE COMPUTER FORENSIC EVIDENCE COLLECTION SYSTEM AND PROCESS



(57) Abstract: The incident response team enters relevant data into a CGI template, i.e. a script. The script then generates an appropriate kernel image for the client machine (10) along with a client folder on the evidence aggregation server. This is where the data is stored, the data about the victim machine. A partition on the evidence aggregation server is also created. The client is also provided orally with a one-time password. The client then connects to the signing authority web site with the one-time password and downloads the kernel boot image onto a storage medium, such as a floppy disk. The disk image is encrypted using an encryption application such as open PGP, and the encrypted image is sent to the client (12). The client inserts the floppy disk that contains the bootable image into the victim machine, and reboots the machine from the floppy disk (14). Data are retrieved from the victim machine, streamed to the evidence aggregation server (18) via an SSL connection, stored at the evidence aggregation server (18) to a hard drive of the victim machine, and processed (16). A message digest is written across the secure connection to a disk on the secure server (24). Hashes are sent to trusted party via the ssl (26 and 28) and compared to the original hash from the compromised machine. Timestamps are also taken and written to the disk on the secure server (18). The disk on the secure server (18) is removed and a chain of custody is created (22). The evidence is stored in a secure location (20).

WO 02/071192 A3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/06622

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : GO6F 11/60
US CL : 713/200

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 155, 200, 201, 202; 711/161, 162, 163, 164

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
N/A

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Dialog and East, Forensic, ambient data, biometrics, copying adj images, suspect or victim

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 5,960, 460 A(MARASCO et al.) 28 SEPTEMBER 1999, see col. 1, lines 66-67, col. 2, lines 1-24, col. 3, lines 52-60, col. 5, lines 4-67, col. 9, lines 13-24.	1-4 ---------- 9
Y	US 6,091,835 A(SMITHES et al.) 18 JULY 2000, see col. 1, lines 1-35, col. 2, lines 41-45, col. 14, lines 22-47, col. 24, lines 1-25.	9
A	US 5,781,629 A(HABER et al.) 14 JULY 1998, see col. 1, lines 64-67, col. 2, lines 1-5.	10
A,P	US 6,263, 349 A B1(ANDERSON) 17 JULY 2001, see col. 1, lines 35-43, col. 7, lines 49-56.	1

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 August 2002 (23.08.2002)	11 SEP 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Gail Hayes FM James R. Matthews Telephone No. (703) 306-0426

Form PCT/ISA/210 (second sheet) (July 1998)