(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 683 218**

(51) Int. CI.:

G06F 3/06 (2006.01)
G11B 5/86 (2006.01)
G06T 11/20 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **05.12.2013 PCT/GB2013/053217**

(87) Fecha y número de publicación internacional: **26.06.2014 WO14096775**

(96) Fecha de presentación y número de la solicitud europea: **05.12.2013 E 13815102 (2)**

(97) Fecha y número de publicación de la concesión europea: **30.05.2018 EP 2941688**

(54) Título: **Sistema y procedimiento de formación de una imagen de memoria digital**

(30) Prioridad:

21.12.2012 GB 201223194
15.01.2013 GB 201300690
26.09.2013 GB 201317136

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.09.2018

(73) Titular/es:

MOBILE CONTENT MANAGEMENT SOLUTIONS LIMITED (100.0%)
Unit 3 Foundry Court Foundry Lane
Horsham, Sussex RH13 5PY, GB

(72) Inventor/es:

FARRELL, PAUL

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema y procedimiento de formación de una imagen de memoria digital

Descripción

La presente invención se refiere a un sistema y un procedimiento de formación de una imagen de memoria digital. En particular, la presente invención se refiere a un sistema para la formación de una imagen de memoria digital para su utilización por personal de la policía, de las fuerzas de seguridad, de inteligencia y militar, y tiene aplicación particular en el sector de la informática forense.

Las investigaciones del personal de la policía, de las fuerzas de seguridad, de inteligencia y militar requieren a menudo la obtención secreta de datos mediante la formación de una imagen de memoria digital, utilizándose a menudo los datos obtenidos como evidencias en futuras actuaciones. El proceso de formación de la imagen toma una imagen "bit a bit" de los datos; por ejemplo, de un disco duro. Es conocido el almacenar la imagen de memoria digital en un dispositivo de memoria extraíble (RMD, removable memory device), tal como una unidad flash USB. Sin embargo, el dispositivo de memoria extraíble tiene un tamaño de almacenamiento limitado y a menudo un solo dispositivo no es suficiente para el proceso requerido de formación de la imagen. Si la imagen de memoria digital es mayor que el tamaño del RMD, no se pueden extraer todos los datos necesarios. Se ha encontrado asimismo que la formación de una imagen de datos en un dispositivo de memoria extraíble es mucho más lenta que la lectura de la memoria digital, lo que puede crear un "cuello de botella" en el proceso de formación de la imagen, de manera que puede no obtenerse la evidencia requerida o se pone en riesgo la naturaleza secreta de la formación de la imagen.

Cuando se intenta formar una imagen de un disco duro en un único dispositivo USB, el usuario se tiene que asegurar de que existe espacio suficiente en el dispositivo USB para almacenar toda la imagen del disco. Por ejemplo, se requieren 80 GB de espacio libre para formar una imagen de un disco duro de 80 GB, independientemente de si está en uso la totalidad de los 80 GB de espacio libre en el disco duro objetivo. Esto se debe a que el proceso de formación de la imagen forma una imagen de todos los archivos y además de todo el espacio libre. Por lo tanto, es común que las investigaciones se queden sin tiempo o sin espacio de almacenamiento para formar la imagen del disco objetivo requerido.

Las herramientas conocidas para la formación forense de una imagen de un PC/portátil en un dispositivo USB son ineficientes y lentas. Las herramientas comunes, tal como Forensic Toolkit® Imager "FTK", proporcionado por la firma AccessData® Group, o EnCase® Forensic Imager, proporcionado por la firma Guidance Software Inc., dependen de que el sistema de formación de la imagen se ejecute desde un dispositivo USB, en el que a continuación se forma la imagen de los datos a través de un único puerto USB. Las herramientas conocidas de formación de una imagen funcionan asimismo desde un "entorno de arranque", de manera que la máquina objetivo cuya imagen se tiene que formar, tiene que ser arrancada utilizando un CD-ROM o un dispositivo USB que contenga una versión editada de un sistema operativo, para permitir que el dispositivo de formación de la imagen acceda a los discos internos de la máquina objetivo. Los CD-ROM de entorno de arranque conocidos incluyen el "Helix-3", proporcionado por la firma e-fense Security Solutions, y el CD de arranque Paladin (marca registrada). La falta de velocidad y la ineficiencia de dichos sistemas conocidos son perjudiciales para la naturaleza secreta de las investigaciones, y a menudo implican que no se pueda formar la imagen de todos los datos requeridos, en particular cuando solamente existe un tiempo disponible muy limitado para obtener los datos.

Además de la ineficiencia de los sistemas conocidos de formación de una imagen, los discos duros son ahora más grandes lo que significa que se tarda más tiempo en formar la imagen de los datos necesarios en dispositivos USB. Es conocido el acoplar a un disco duro un generador de imágenes de disco especializado, tal como el "Tableau TD1 Forensic Duplicator" proporcionado por la firma Guidance Software Inc., que permite que la imagen del disco duro se genere más rápidamente. Sin embargo, esto requiere tiempo y es inoportuno llevar a cabo la extracción y el reemplazo necesarios del disco duro desde la máquina que debe ser investigada, para permitir que tenga lugar la formación de la imagen TD1. Si existe el tiempo y la oportunidad para extraer el disco duro durante la investigación, esto puede suponer habitualmente desde 20 minutos hasta varias horas, además del tiempo necesario para reinstalar el disco duro después de la formación de la imagen. Por lo tanto, cuando se requiere que las investigaciones se lleven a cabo en un tiempo muy limitado, a menudo solamente es posible obtener una imagen parcial del disco duro y no se capturan pruebas decisivas. Además, cada vez es más común que no sea posible extraer el disco duro para permitir que tenga lugar la formación de la imagen con estos dispositivos conocidos. Por ejemplo, el disco duro está situado detrás de una pantalla o enterrado en los componentes electrónicos del propio ordenador. El disco duro puede asimismo estar unido al ordenador o tener etiquetas de seguridad para indicar que el disco ha sido forzado. Esto no sólo hace difícil y prolongada la extracción, sino que implica un riesgo de que se descubra una operación secreta cuando es fundamental que el ordenador se quede en un estado idéntico para que la investigación del ordenador no pueda ser detectada.

La publicación de patente de EE.UU. número US2006/0164743 da a conocer un procedimiento de copia de uno-a-varios, de un medio de almacenamiento de datos, en el que los datos de origen en un disco duro se copian a una serie de discos duros uno por uno. Es bien conocido que dichos procedimientos permiten leer y almacenar conjuntamente todo el disco duro de un ordenador personal en cada uno de una serie de discos duros. El objetivo de

dichos procedimientos es proporcionar muchas copias del disco duro de origen, u objetivo. Para su utilización en las investigaciones, el objetivo principal de un procedimiento de este tipo es crear simultáneamente una copia que se mantendrá como la 'copia probatoria', y otras copias para distribuir a uno o varios miembros del personal a través de equipos. De este modo, los datos en forma de imagen están disponibles para que múltiples personas los investiguen y analicen, de tal modo que aumenta la velocidad del proceso de investigación. Además, el procedimiento dado a conocer en la patente de US 2006/0164743 alivia el problema de los problemas de hardware en los discos duros cuando se forma la imagen de los datos, que constituye el punto de fallo más probable en un proceso de copia de disco duro. En una operación secreta, una copia directa de este tipo es, en realidad, prolongada e ineficiente. Cuando un usuario necesita que el disco duro objetivo se copie solamente una vez de la manera más rápida y precisa posible, este procedimiento no proporciona una solución adecuada. El procedimiento de la patente US 2006/0164743 requiere asimismo la extracción del disco duro desde el ordenador, provocando los problemas discutidos anteriormente.

Además, completar el proceso de formación de la imagen de cualquier memoria digital requiere a menudo un considerable periodo de tiempo, por ejemplo, varias horas consecutivas. La naturaleza secreta de la investigación hace a menudo improbable que este periodo de tiempo necesario esté disponible. Los sistemas existentes de formación de una imagen de memoria digital, que no están concebidos para investigación secreta, son tales que si no está disponible el tiempo completo necesario entonces no se puede conseguir satisfactoriamente la formación de la imagen de la memoria digital. Por ejemplo, si un usuario desea formar una imagen de un disco duro de 80 GB pero es interrumpido en mitad del tiempo necesario para completar la adquisición de una imagen de 80 GB, no hay entonces ni ningún dato de en forma de imagen que el usuario se pueda llevar.

La publicación de patente de EE.UU. número US2007/0043967 da a conocer una reconexión y adquisición automáticas en un sistema de investigación informática. El sistema es para ser utilizado en una red de ordenadores. Cuando se pierde la conexión durante la adquisición de datos desde la red, el ordenador examinador puede intentar automáticamente la reconexión del sistema de investigación, y una vez se ha restablecido la conexión la máquina objetivo continúa la adquisición desde un estado intermedio, es decir, desde el momento en que se perdió la conexión. El sistema de la patente US2007/0043967 no es adecuado para su utilización en investigaciones secretas dado que requiere un permiso previo para que el usuario se conecte a la red de ordenadores y tenga acceso autorizado. Este sistema es adecuado solamente para obtener datos desde una red (y donde el ordenador objetivo está ejecutando manifiestamente el software cliente de formación de una imagen), no para la formación de una imagen de datos digitales directamente en un dispositivo de memoria extraíble, tal como un USB.

La publicación de patente de EE.UU. número US2004/0260733 da a conocer una técnica para obtener remotamente y analizar informática forense y está relacionada con la reducción del impacto sobre el dispositivo informático objetivo. La patente US2004/0260733 da a conocer una solución alternativa a la inspección in situ del ordenador objetivo utilizando la conexión física de un dispositivo de análisis, mediante la disposición de un dispositivo forense acoplado a un ordenador objetivo mediante un enlace de comunicaciones, utilizando un sistema basado en web y una interfaz basada en red. La patente US2004/0260733 determina un orden para llevar a cabo operaciones de adquisición con el fin de reducir el impacto de la adquisición de datos sobre los datos almacenados en el ordenador objetivo.

La patente de EE.UU. número US 7.181.560 da a conocer un procedimiento de conservación de evidencias digitales para ser utilizado por un investigador forense, que involucra almacenar una imagen de memoria en un único disco de almacenamiento externo extraíble utilizando un único sistema de cola.

La presente invención se presenta para aliviar los problemas descritos anteriormente, dando a conocer un sistema y un procedimiento de formación de una imagen de memoria digital con mayor eficiencia, que permiten una extracción de datos rápida y segura.

En un aspecto, la presente invención da a conocer un sistema de formación de una imagen de memoria digital para la formación de una imagen de la memoria digital de un ordenador objetivo, tal como se define en la reivindicación 1.

En otro aspecto, la presente invención da a conocer un procedimiento de formación de una imagen digital para formar una imagen de la memoria digital de un ordenador objetivo, según se define en la reivindicación 7.

Para una mayor claridad y para una descripción concisa, las características se describen en la presente memoria como parte de las mismas realizaciones o de realizaciones independientes; sin embargo, se apreciará que el alcance de la tecnología puede incluir realizaciones con combinaciones de todas o parte de las características descritas.

Estas y otras características de la presente tecnología se comprenderán mejor haciendo referencia a la siguiente descripción detallada junto con los dibujos adjuntos, en los cuales:

la figura 1 es un diagrama de bloques de un ejemplo del sistema de formación de una imagen de memoria digital construido de acuerdo con la presente invención;

la figura 2a es un diagrama de flujo del procedimiento de formación de una imagen de memoria digital de una primera realización de la presente invención;

la figura 2b es un diagrama de flujo del ingreso en cola dinámico llevado a cabo por el procedimiento de formación de una imagen de memoria digital de una primera realización de la presente invención;

la figura 3 es un diagrama de flujo del procedimiento de formación de una imagen de memoria digital de una realización alternativa de la presente invención; y

la figura 4 es un gráfico que ilustra la prueba detallada en el apéndice 2, que muestra velocidad de transferencia frente a tamaño de memoria tampón de lectura, para varios tamaños de memoria tampón de escritura en un sistema típico de "gama media".

Las figuras descritas en la presente memoria, en la totalidad de las cuales las partes semejantes se indican mediante numerales de referencia, muestran realizaciones de ejemplo de un procedimiento y un sistema de formación de una imagen de memoria digital de acuerdo con la presente tecnología. Aunque la presente tecnología se describirá haciendo referencia a las realizaciones de ejemplo mostradas en las figuras, se debe entender que muchas formas alternativas pueden incorporar la presente tecnología.

Haciendo referencia a la figura 1 y a un ejemplo del sistema de formación de una imagen de memoria digital, el ordenador objetivo 1 puede recibir múltiples dispositivos extraíbles de almacenamiento de datos, incluyendo cualquier combinación de unidades 3 de USB 1.0, USB 2.0 y 3.0; dispositivos externos eSata 5; tarjetas SD y microSD 7; unidades FireWire (marca registrada) 9; unidades Thunderbolt (marca registrada) 11 y unidades externas PCI Express 13. Se entiende que el ordenador objetivo es un ordenador personal, un portátil, un ordenador de tableta o cualquier dispositivo similar que se pueda conectar a un dispositivo extraíble de almacenamiento de datos.

Un usuario con acceso al ordenador objetivo 1 introduce el sistema de formación de una imagen de memoria digital en el ordenador objetivo 1 mediante la unidad USB 1.0, 2.0 o 3.0, 3, o un dispositivo similar, 5, 7, 9, 11, 13. Una unidad USB 3 se conecta al ordenador objetivo 1 y actúa como un dispositivo "anfitrión" para permitir que se lleve a cabo el procedimiento de formación de una imagen de memoria digital.

Haciendo referencia a la figura 2a, en una realización preferida del procedimiento de formación de una imagen de memoria digital, el sistema de formación de una imagen de memoria digital se conecta al ordenador objetivo en la etapa 200 y se inicia el procedimiento de formación de la imagen de memoria digital. En la etapa 201, el sistema detecta los dispositivos de almacenamiento de datos, es decir, los dispositivos físicos determinados de (unidad de) memoria digital en los que se va a formar la imagen de la memoria digital del ordenador objetivo. Por ejemplo, en la etapa 201, el sistema detecta que tres dispositivos USB 2.0, dos dispositivos USB 3.0 y una tarjeta PCIe USB 3.0 están introducidos en el ordenador objetivo. En la etapa 203, el sistema excluye el dispositivo de almacenamiento anfitrión; por ejemplo, el dispositivo extraíble de almacenamiento de datos USB 2.0, USB 3.0 o similar en el que está almacenado el sistema de formación de la imagen. Por lo tanto, en el ejemplo anterior, el sistema detecta que un dispositivo USB 2.0 contiene el sistema de formación de una imagen de memoria digital y que se tienen que utilizar dos dispositivos USB 2.0 restantes, dos dispositivos USB 3.0 y una tarjeta PCIe USB 3.0 para formar la imagen del disco duro (memoria digital) del ordenador objetivo. Se entiende que la referencia al disco duro incluye cualquier clase de memoria digital, tal como una memoria flash o una memoria de acceso aleatorio (RAM, random access memory). Simultáneamente, en la etapa 205, el sistema detecta las unidades lógicas, es decir, la memoria digital del ordenador objetivo.

En la etapa 207, el sistema recopila y muestra los dispositivos y las unidades que ha detectado previamente. Por ejemplo, la información se visualiza en la pantalla del ordenador objetivo. En la etapa 209, un usuario ordena al sistema que comience la formación de la imagen de la memoria digital objetivo.

El sistema comienza a continuación a formar la imagen de la memoria digital objetivo mediante leer secuencialmente la memoria en grandes bloques de datos. El tamaño de los bloques de datos está predeterminado para garantizar un rendimiento óptimo para tipos comunes de dispositivos. Se ha descubierto que un tamaño de bloque de 8 MB permite un equilibrio óptimo entre la capacidad de memoria del ordenador que lleva a cabo el procedimiento y la longitud de la cola para almacenar los bloques de datos a través de los múltiples dispositivos de memoria extraíble. Por ejemplo, un ordenador personal pequeño tiene una memoria de aproximadamente 512 MB, y un tamaño de bloque de datos de 8 MB es lo suficientemente pequeño como para no sobrecargar un ordenador objetivo con memoria de este tamaño, mientras que el bloque de datos de 8 MB es lo suficientemente grande como para que la utilización de la unidad central de procesamiento (CPU, central processing unit) sea fundamentalmente en tiempo del núcleo, de tal modo que el procesamiento es lo más eficiente posible.

Haciendo referencia a las etapas 211, 213, 215, el sistema avanza de tal modo que a medida que se lee cada bloque de datos de la memoria digital objetivo en la etapa 211, se forma su imagen y esta se asigna para almacenamiento en uno de los dispositivo de memoria extraíble (RMD) detectados. La asignación se determina en función de un sistema de cola jerárquico. Cada dispositivo de memoria extraíble tiene una cola de datos que tiene que almacenar. El tamaño del bloque de datos preferido de 8 MB se selecciona para que sea compatible con la longitud de la cola con el fin de evitar inactividad en la salida. En la etapa 213, cada bloque de datos que se lee es

asignado a la cola RMD más corta. Por lo tanto, cada bloque de datos se asigna al RMD que tiene actualmente la mínima cantidad de datos para almacenar y/o al RMD con la mayor velocidad. Esto garantiza una eficiencia de almacenamiento máxima a través de los múltiples dispositivos de memoria extraíble. El sistema de colas es dinámico, de manera que la cola de cada dispositivo de memoria extraíble es monitorizada constantemente.

Haciendo referencia a la figura 2b, la asignación de cada bloque de datos comienza en la etapa 222, antes de que el sistema lea el bloque de datos en la etapa 224. En la etapa 226, el sistema selecciona el siguiente dispositivo de salida RMD y pregunta en la etapa 228 si el dispositivo tiene la más corta de las colas. Si en la etapa 230 se detecta que el dispositivo tiene la más corta de las colas, el bloque de datos se añade a dicha cola, es decir, para ser almacenado en ese RMD. Sin embargo, si en la etapa 228 el RMD no tiene la más corta de las colas, el sistema avanza a la etapa 226 para seleccionar el siguiente RMD en la lista y volver a preguntar, en la etapa 228, si el dispositivo tiene la más corta de las colas.

Cuando el sistema ha repetido las etapas necesarias hasta llegar al RMD con la más corta de las colas, comprueba en la etapa 230 si la cola es lo suficientemente corta como para permitir el almacenamiento eficiente del bloque de datos. Si la cola no es lo suficientemente corta y es probable que la adición del bloque de datos afecte a la eficiencia del sistema, en la etapa 232 se retrasa la adición del bloque de datos. Si la cola es lo suficientemente corta, el bloque de datos se añade a la cola del RMD seleccionado, en la etapa 234. En la etapa 236, el sistema de colas dinámico sigue asignando cada bloque de datos del mismo modo hasta que se ha formado y almacenado la imagen de todos los datos, y el procedimiento finaliza en la etapa 238.

Haciendo referencia a la figura 2a, la lectura, la formación de la imagen y el almacenamiento de la memoria digital del ordenador objetivo continúa hasta que no existen más datos a leer y en la etapa 215 se detecta el fin del archivo (EOF, end of the file). Por lo tanto, el proceso de formación de la imagen continúa hasta que se ha formado una imagen de toda la memoria objetivo, y el procedimiento finaliza en la etapa 220.

Simultáneamente a los procesos de lectura y almacenamiento de la formación de la imagen, 211, 213, 215, el sistema detecta en la etapa 217 si alguno de los dispositivos de almacenamiento de datos (RMD) está lleno. La detección de un dispositivo de almacenamiento de datos lleno se indicará a un usuario por medio de la pantalla del sistema. Esto proporciona al usuario la oportunidad de retirar el dispositivo lleno y sustituirlo con un nuevo RMD con capacidad de almacenamiento. El sistema detecta asimismo en la etapa 217 si un nuevo dispositivo de almacenamiento de datos es introducido, o si un dispositivo de almacenamiento de datos lleno es extraído o desconectado del ordenador objetivo. El sistema no limita el número de extracciones/desconexiones o introducciones/conexiones de dispositivos de almacenamiento de datos en un mismo proceso de formación de la imagen. Por lo tanto, no existe ningún límite sobre la cantidad de datos de los que se puede formar una imagen mediante el sistema de la presente invención.

Tal como se muestra en la figura 2a, el proceso de formación de la imagen es continuo hasta que se ha formado la imagen de toda la memoria digital del ordenador objetivo. Durante la formación de la imagen, el volumen de los datos cuya imagen se ha formado y la cantidad restante de datos cuya imagen se tiene que formar se monitorizan para evitar cualesquiera insuficiencias en la capacidad de la memoria o cualquier consiguiente reducción en la velocidad de transferencia de los datos. En otras realizaciones de la invención, se inicia un "estrangulamiento de la lectura" y una "recogida de basura" a intervalos durante el proceso de formación de la imagen cuando dichos procesos han mostrado ser más eficaces. El estrangulamiento de la lectura se inicia siempre que la más corta de las colas de salida de los RMD contiene 20 elementos. La recogida de basura se realiza al mismo tiempo, cuando el sistema operativo no puede suministrar una nueva memoria tampón.

En la etapa 220, cuando el proceso de formación de la imagen se ha completado, los datos que se han recogido serán convertidos a un archivo de imagen. La interfaz de usuario proporciona pantallas adecuadas para solicitar al usuario el inicio de la conversión.

Haciendo referencia a la figura 2a y a la etapa 211, los datos objetivo cuya imagen se tiene que formar se leen en bloques. Cada bloque de datos comprende una cabecera de 4096 octetos, seguida por el segmento de datos cuya imagen se tiene que formar. La cabecera comprende información a modo de cadena de texto, con los campos siguientes:

i) Número secuencial del bloque de datos: (0, 1, 2, 3....n);

ii) Longitud de los datos: cómputo de octetos del segmento de datos.

iii) Valor de compresión: si este valor es cero, entonces los datos están sin comprimir. Si este valor es distinto de cero, hace referencia a la técnica utilizada para comprimir el segmento de fechas. En las realizaciones preferidas de la presente invención, la compresión se lleva a cabo con un algoritmo "gzip";

iv) Dirección de origen: la dirección en el dispositivo de memoria objetivo desde la que se extrajo el bloque de datos;

v) Marca de tiempo: indica cuándo se inició la formación de la imagen de los datos;

vi) Identificador único de la ronda de recogida de datos: un identificador único global (GUID, Globally Unique Identifier) de 16 octetos generado al comienzo del proceso de recogida de datos:

El número secuencial y el valor de compresión se utilizan cuando se de combinan los datos cuya imagen se ha formado, en la etapa 220, para formar un archivo de imagen de la memoria digital objetivo. La marca de tiempo y el identificador único permiten validar los datos en forma de imagen.

En una realización alternativa de la presente invención, si un usuario no tiene acceso a un dispositivo "anfitrión" que contiene el sistema de formación de una imagen de memoria digital, el procedimiento incluye una etapa adicional anterior a la etapa 201, en la que un dispositivo USB vacío es conectado al ordenador objetivo y el sistema de formación de una imagen de memoria digital es descargado a través de internet. Las instrucciones sobre cómo descargar el sistema se proporcionan por separado respecto del USB, o alternativamente se proporcionan en el USB instrucciones breves en relación con el acceso a la descarga. Se contempla que, en una realización preferida, un usuario será autorizado a acceder al sistema o recibirá permiso para descargar el sistema, por medio de una licencia proporcionada en un dispositivo USB. A continuación, el usuario podrá validar múltiples dispositivos extraíbles de almacenamiento de datos en función de sus necesidades.

Tal como se ilustra mediante los resultados de pruebas mostrados en el apéndice 1, la velocidad de formación de la imagen se incrementa dividiendo de manera efectiva el proceso de formación de la imagen a través de múltiples dispositivos de almacenamiento de datos conectados a la máquina objetivo. Los dispositivos de almacenamiento de datos se pueden introducir en cada uno de los puertos siguientes, en cualquier combinación: USB 1.0; USB2.0; USB3.0; PCIe; ranuras de tarjeta; ranuras de tarjeta SD; FireWire (marca registrada) de Apple (marca registrada) y Thunderbolt (marca registrada) de Apple (marca registrada). Con múltiples dispositivos de almacenamiento de datos conectados a la máquina objetivo, la imagen de la unidad se divide de manera efectiva a través de los diferentes puertos y por lo tanto de diferentes canales BUS de la placa base. Esto aumenta la velocidad y la eficiencia de la formación de la imagen y permite asimismo que el tamaño de la unidad objetivo se divida a través de varios dispositivos de almacenamiento de datos.

Haciendo referencia a la figura 3 y a una realización alternativa del sistema de formación de la imagen de la presente invención, el procedimiento descrito anteriormente se puede llevar a cabo en múltiples sesiones debido a que el procedimiento incluye la opción de comenzar y detener el proceso a conveniencia. La realización alternativa mostrada en la figura 3 permite al usuario parar el procedimiento de formación de la imagen y almacenar resultados antes de reanudar el procedimiento de formación de la imagen , es decir, el sistema queda "suspendido en espera". En la etapa 300, el proceso de formación de la imagen se inicia, y en la etapa 301 el sistema crea un archivo de registro correspondiente a la posición actual cuya imagen se está formando, y la posición se almacena en el archivo de registro. En la etapa 302, el sistema crea un archivo de imagen maestro, en el que los datos en forma de imagen serán almacenados. En la etapa 303, antes de que comience la formación de la imagen, se ajusta la posición actual de la memoria digital al comienzo.

En la etapa 304, el proceso de formación de la imagen comienza a formar la imagen de la memoria digital del ordenador objetivo, y los resultados de la imagen se almacenan en un archivo de trabajo. La posición de la memoria digital se incrementa y se indexa, y el archivo de registro se actualiza a medida que progresa la formación de la imagen. Por ejemplo, en un entorno de ventanas, cada octeto en una unidad de disco o en un dispositivo de estado sólido (SSD, solid state device) se indexa como un número consecutivo a partir de cero, utilizándose números consecutivos en varios intervalos separados para indexar cada octeto en RAM. En la etapa 305, el sistema monitoriza si se ha interrumpido el proceso de formación de la imagen. Se produce una interrupción, en la etapa 306 el sistema monitoriza si se ha reanudado el proceso. Después de una interrupción, en la etapa 307, cuando el proceso se reanuda se utiliza un archivo de registro para dirigir al sistema para que reanude el proceso de formación de la imagen desde el punto de interrupción.

El procedimiento de formación de la imagen continúa hasta que, en la etapa 308, el archivo de imagen de trabajo está lleno. En la etapa 309, el archivo de trabajo se añade al archivo de imagen maestro y el archivo de imagen de trabajo se borra. La etapa 310 incrementa a la posición de la memoria digital y el archivo de trabajo se actualiza en consecuencia. Este proceso de actualización del archivo de trabajo y comprobación de las interrupciones continúa hasta que, en la etapa 311, el sistema llega al final de la memoria digital objetivo o el usuario detiene el proceso. El proceso finaliza en la etapa 312. Si el usuario detiene el proceso, el resultado de la imagen en el archivo de trabajo actual se ignora y el usuario habrá formado la imagen de solamente parte de la memoria digital objetivo. Si se desea se pueden utilizar múltiples archivos de imagen maestros, y cuando un archivo de imagen maestro alcanza un tamaño predeterminado se crea un nuevo archivo de imagen maestro. Esto permite al usuario reunir una parte de la memoria digital en cualquier sesión, y formar la imagen de toda la memoria digital durante múltiples sesiones.

Las realizaciones descritas anteriormente se han proporcionado solamente a modo de ejemplo, y por supuesto el lector experto en la materia apreciará que se podrían realizar en las mismas muchas variaciones sin apartarse del alcance de las reivindicaciones.

Cualesquiera valores proporcionados en la presente memoria son ilustrativos y no limitan en modo alguno la presente invención. Tras la lectura de la presente memoria descriptiva, un experto en la materia apreciará que se

puede utilizar una gran variedad de otros parámetros para implementar el sistema y el procedimiento de formación de una imagen de memoria digital. La totalidad de dichas alternativas y modificaciones se contemplan dentro del alcance de la presente invención, tal como se define mediante las reivindicaciones.

Resultarán evidentes para los expertos en la materia numerosas modificaciones y realizaciones alternativas de la presente invención, a la luz de la descripción anterior.

Se debe entender asimismo que las siguientes reivindicaciones tienen que abarcar todas las características genéricas y específicas de la invención descrita en la presente memoria, y todas las declaraciones del alcance de la invención que, por cuestiones de lenguaje, se puede decir que quedan entre estas.

Apéndice 1

A modo de comparación, para mostrar la mayor velocidad y eficiencia de la presente invención, en la tabla 1 se exponen datos experimentales del tiempo que se ha tardado en formar una imagen de un disco duro objetivo utilizando un único puerto USB empleando la tecnología conocida de formación de una imagen, FTK Imager v3 1.3.2 Forensic Toolkit® Imager, proporcionada por la firma AccessData® Group, con la unidad acoplada a un dispositivo Tableau TD1 Forensic Duplicator proporcionado por la firma Guidance Software, Inc.

Portátil	Disco duro	CPU	RAM (GB)	Tableau TD1 Drive Imager		FTK Imager (USB 2.0)		FTK Imager (USB 2.0	
				Tiempo hasta la imagen (min)	Velocidad (GB/min)	Tiempo (min)	Velocidad (GB/min)	Tiempo (min)	Velocidad (GB/min)
Prueba 1									
Dell Latitude (marca registrada) E6230	Hitachi HTS7250 32A7E63 0 320 GB 7200 rpm	Procesador Core i5 3380M	4	76	4,211	230,0 5	1,391	82,13	3,89 6
Prueba 2									
Dell Alienware M18x	Samsung PM830 256 GB SSD	Procesador Core i7 3920XM a 3,1 GHz	16	50,55	5,064	Sin puertos USB 2,0	40,85	6,26 7	
Prueba 3									
Dell Vostro 3450	Samsung HM320HJ 320 GB 7200rpm	Procesador Core i5 2410Ma 2,3 GHz	4	77,80	4,113	224	1,42 9	84,58	3,78 3

[Tabla 1]

La tabla 2 presenta datos experimentales del tiempo que lleva formar una imagen de un disco duro objetivo utilizando el sistema y el procedimiento de formación de una imagen de memoria digital de la presente invención, utilizándose los diversos puertos para hacer uso de una combinación de dispositivos de almacenamiento de datos conectados a la máquina objetivo.

Portátil	Disco duro	CPU	RAM (GB)	Portátil de rendimiento encendido		Portátil de rendimiento apagado		
				Tiempo hasta la imagen (min)	Velocidad (GB/min)	Tiempo (min)	Velocidad (GB/min)	Puertos utilizados
Prueba 1								
Dell Latitude (marca registrada) E6230	Hitachi HTS7250 32A7E63 0 320 GB 7200 rpm	Procesador Core i5 3380M	4	75,98	4,212	69,52	4.604	1 x USB2.0 2 x USB3.0
Prueba 2								
Dell Alienware M18x	Samsung PM830 256 GB SSD	Procesador Core i7 3920X M a 301GHz	16	11,33	22,59	13,52	18,94	2 x USB3.0 1 x eSATA
Prueba 3								
Dell Vostro 3450	Samsung HM320HJ 320 GB 7200rpm	Procesador Core i5 2410M a 2.3G Hz	4	58,52	5,469	73,00	4,385	2 x USB2.0 2 x USB3.0 1 x tarjeta PCIe USB3.0

[Tabla 2]

Comentarios sobre los resultados de las pruebas

Se puede ver que la presente invención aumenta la velocidad y reduce el tiempo que se tarda en la formación de la imagen de los datos.

Con los dispositivos de estado sólido (SSD), los aumentos en la velocidad de la formación de la imagen ofrecida por la presente invención son significativos. Las pruebas detalladas en la presente memoria muestran una velocidad de formación de la imagen que es aproximadamente de 4 a 5 veces más rápida que los dispositivos conocidos.

Haciendo referencia a la prueba 2, realizada para una unidad SSD, el sistema TD1 de la técnica anterior formó una imagen del dispositivo en 50 minutos 33 segundos a una velocidad de 5,064 GB/min; el sistema FTK de la técnica anterior formó una imagen de la unidad en 40 minutos 51 segundos a una velocidad de 6,267 GB/min. El sistema de formación de la imagen de la presente invención formó una imagen de la unidad de 11 minutos y 20 segundos, a la velocidad mucho más rápida de 22,59 GB/min.

El aumento en la velocidad de formación de la imagen se añade al tiempo ganado gracias a que la presente invención no requiere que la unidad sea extraída del ordenador objetivo, es decir, el sistema de la presente invención permite la formación de la imagen de la memoria digital del ordenador objetivo manteniendo la unidad SSD in situ en el ordenador. Para permitir la formación de la imagen de una unidad giratoria, es decir de una unidad no SSD, el sistema TD1 de la técnica anterior requiere que el disco duro sea extraído del ordenador objetivo y acoplado al generador de imágenes TD1 para que tenga lugar la formación de la imagen. La extracción requiere habitualmente por lo menos 20 minutos además del tiempo requerido para la formación de la imagen. A continuación es necesario reinstalar la unidad sin dejar signos de su extracción/reinstalación. Algunos sistemas informáticos tienen sus unidades de disco situadas detrás de pantallas o situadas en otras áreas inaccesibles o, de hecho, con precintos anti-manipulación, etc., que hacen imposible la extracción/reinstalación en investigaciones secretas.

Haciendo referencia a la prueba 3, realizada para una unidad no SSD, basada en plato, el sistema TD1 de la técnica anterior formó una imagen de la unidad en 77 minutos 48 segundos a una velocidad de 4,113 GB/min y requirió 40 minutos para la extracción de la unidad desde el ordenador objetivo y su reinstalación en el mismo. La presente

invención formó la imagen de la unidad en 58 minutos 31 segundos a una velocidad de 5,469 GB/min, sin necesidad de extraer la unidad del ordenador objetivo.

La prueba 3 muestra asimismo que la adición de una tarjeta PCIe Express adicional aumenta la capacidad del USB 3.0 y aumenta la velocidad de la formación de la imagen y por lo tanto la eficiencia de la extracción de los datos desde el dispositivo objetivo.

En conclusión, se ha mostrado que el sistema y el procedimiento de formación de imagen de la presente invención ofrecen una velocidad de formación de la imagen significativamente mayor, de tal modo que se requiere un tiempo de formación de la imagen significativamente menor.

Apéndice 2

Para optimizar la formación de la imagen de la memoria digital objetivo, se llevaron a cabo pruebas de la velocidad de transferencia para tamaños variables de la memoria tampón de lectura y de la memoria tampón de escritura, en un sistema típico de gama media. El sistema comprendió un disco Western Digital "Green" 5400 RPM de 8 GB de memoria y cuatro puertos USB 2.0. La prueba se llevó a cabo sobre la misma máquina variándose solamente el tamaño de la memoria tampón entre las pruebas. Los resultados de esta prueba se resumen en [la tabla 3]:

	Tamaño de escritura:										
Tamaño de lectura:	0,031	0,06	0,125	0,25	1	1,5	2	3	4	8	32
0,031			10,98	14,33	75,89	17,52	16,06		16,48		23,87
0,125	51,4	51,5			73,69			19,08		20,75	
1	76,14		77,2	75,42	28				21,27		
2		76,87	79,22	78,62	77,13	77,69	26,94	25,55			19,6
3			77,93	77,53			77,78	27,13			
4	76,2				78,15		77,4	76,33	29		
6						77,89	77,99	78,2	77,47		
8	77,18		76,4	76,1	78,5		77,93	75,92	77,9	27,1	26,1
10							77,8				
12		78,22					79,16	78,32			
16	75,79	80,63	80,14	79,22	76,27	77,21	79,3	78,82	77,81	76,24	32,29

[Tabla 3]

Comentarios sobre los resultados de las pruebas

A partir de esta prueba se concluyó que siempre que el tamaño de la memoria tampón de lectura sea un múltiplo del tamaño de la memoria tampón de escritura, la velocidad de transferencia es satisfactoria.

REIVINDICACIONES

1. Un sistema de formación de una imagen de memoria digital para la formación de una imagen de la memoria digital de un ordenador objetivo (1), que comprende:

una serie de dispositivos extraíbles de almacenamiento de datos (3, 5, 7, 9, 11, 13), cada uno de los cuales puede ser recibido para ser conectable al ordenador objetivo (1);

un medio de formación de imagen configurado para formar una imagen de la memoria digital del ordenador objetivo (1);

un medio de salida, para entregar la memoria digital en forma de imagen, como una serie de bloques de datos a dos o más de los dispositivos extraíbles de almacenamiento de datos (3, 5, 7, 9, 11, 13); y

un medio de asignación configurado para asignar cada bloque de datos de memoria digital en forma de imagen, a un dispositivo extraíble de almacenamiento de datos seleccionado (3, 5, 7, 9, 11, 13), de acuerdo con un sistema de colas, en el que cada dispositivo extraíble de almacenamiento de datos (3, 5, 7, 9, 11, 13) tiene una cola de datos para almacenar que es monitorizada constantemente, en el que cada bloque de datos es asignado al dispositivo extraíble de almacenamiento de datos que tiene la mínima cantidad de datos para almacenar en su cola.

2. Un sistema de formación de una imagen de memoria digital según la reivindicación 1, en el que la serie de dispositivos extraíbles de almacenamiento de datos comprende cualquier combinación de un USB (3); una unidad externa eSata (5); una tarjeta SD (7); una tarjeta microSD (7).

3. Un sistema de formación de una imagen de memoria digital según cualquier reivindicación anterior, que comprende además un medio de visualización.

4. Un sistema de formación de una imagen de memoria digital según cualquier reivindicación anterior, que comprende además un medio de etiquetado para etiquetar cada bloque de datos en forma de imagen con una cabecera que comprende cualquier combinación de un número secuencial; una longitud de bloque de datos; una dirección de origen, un valor de compresión; una marca de tiempo; un identificador único.

5. Un sistema de formación de una imagen de memoria digital según cualquier reivindicación anterior, que comprende además un medio de almacenamiento, en el que el medio de almacenamiento reacciona a una interrupción de la formación de la imagen de la memoria digital para almacenar la memoria digital en forma de imagen en el punto de interrupción.

6. Un sistema de formación de una imagen de memoria digital según cualquier reivindicación anterior, en el que cada bloque de datos se asigna al dispositivo extraíble de almacenamiento de datos que tiene la mínima cantidad de datos para almacenar y la máxima velocidad.

7. Un procedimiento de formación de una imagen de memoria digital para la formación de una imagen de la memoria digital de un ordenador objetivo, que comprende las etapas de

conectar una serie de dispositivos extraíbles de almacenamiento de datos al ordenador objetivo, de manera que el ordenador objetivo recibe cada uno de los dispositivos de almacenamiento de datos;

formar una imagen de la memoria digital del ordenador objetivo (209, 211);

entregar la memoria digital en forma de imagen, como una serie de bloques de datos a dos o más de los dispositivos extraíbles de almacenamiento de datos; y

asignar (213) cada bloque de datos de la memoria digital en forma de imagen a un dispositivo extraíble de almacenamiento de datos seleccionado, de acuerdo con un sistema de colas, en el que cada dispositivo extraíble de almacenamiento de datos tiene una cola de datos a almacenar que es monitorizada constantemente, en el que cada bloque de datos de memoria digital en forma de imagen se asigna según el dispositivo extraíble de almacenamiento de datos que tenga la mínima cantidad de datos a almacenar en su cola.

8. Un procedimiento de formación de una imagen de memoria digital según la reivindicación 7, que comprende además la etapa de visualizar información de progreso relativa al sistema de formación de la imagen.

9. Procedimiento de formación de una imagen de memoria digital según la reivindicación 7 u 8, que comprende además la etapa (213) de etiquetar cada bloque de datos en forma de imagen, con una cabecera que comprende cualquier combinación de un número secuencial; una longitud de bloque de datos; una dirección de origen; un valor de compresión; una marca de tiempo; un identificador único.

10. Un procedimiento de formación de una imagen de memoria digital según las reivindicaciones 7 a 9, que comprende además la etapa (304, 305, 307, 309) de almacenar la memoria digital en forma de imagen, en un punto de interrupción.

11. Un procedimiento de formación de una imagen de memoria digital según las reivindicaciones 7 a 10, donde el o cada bloque de datos de la memoria digital en forma de imagen es asignado según la memoria libre disponible en cada dispositivo extraíble de almacenamiento de datos y la velocidad del dispositivo extraíble de almacenamiento de datos.

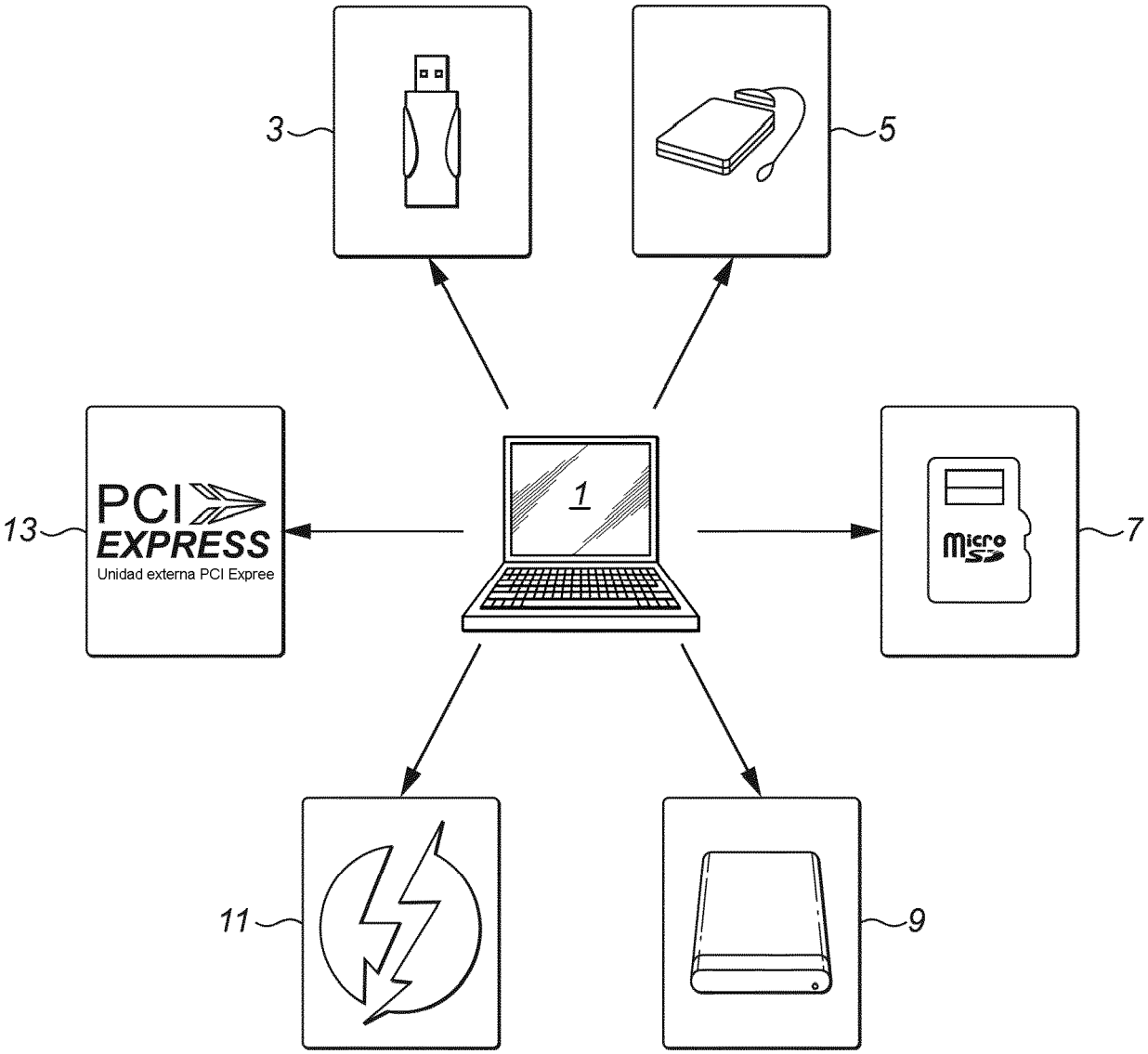

FIG. 1

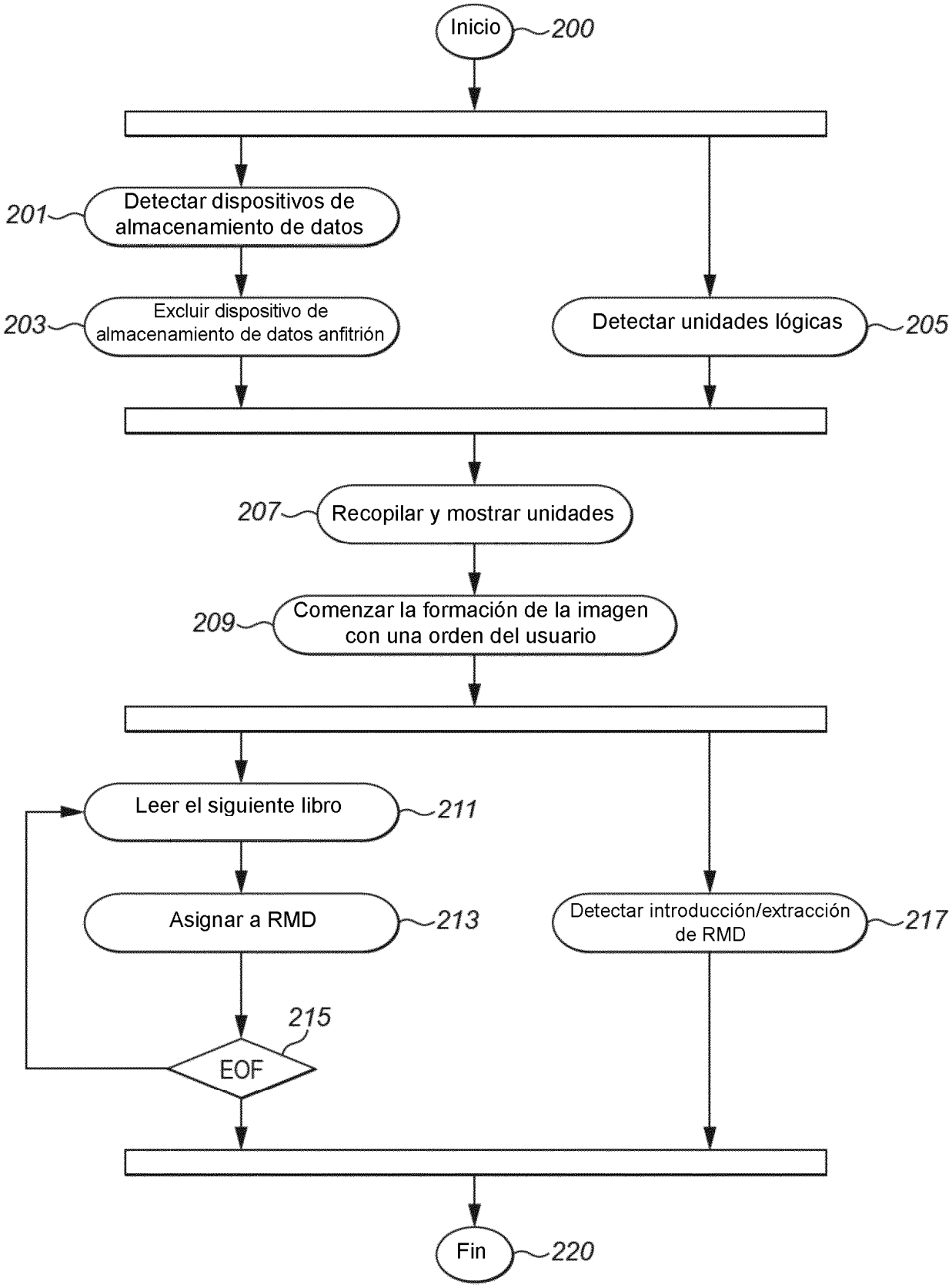
Inicio
200
201
Detectar dispositivos de almacenamiento de datos
203
Excluir dispositivo de almacenamiento de datos anfitrión
Detectar unidades lógicas
205
207
Recopilar y mostrar unidades
209
Comenzar la formación de la imagen con una orden del usuario
Leer el siguiente libro
211
Asignar a RMD
213
Detectar introducción/extracción de RMD
217
215
EOF
Fin
220

FIG. 2a

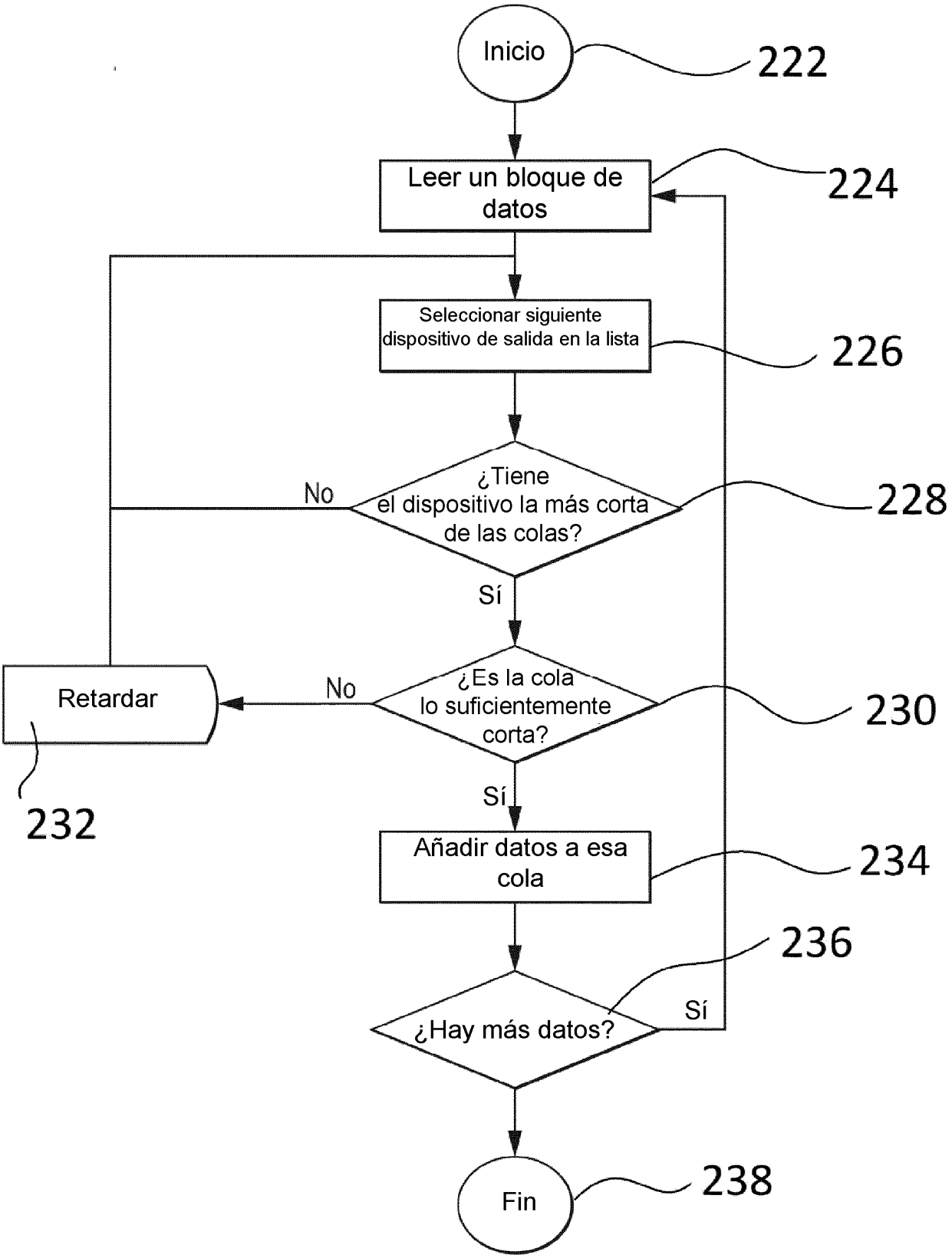
Inicio
222
Leer un bloque de datos
224
Seleccionar siguiente dispositivo de salida en la lista
226
¿Tiene el dispositivo la más corta de las colas?
No
228
Sí
¿Es la cola lo suficientemente corta?
No
230
Retardar
232
Sí
Añadir datos a esa cola
234
236
¿Hay más datos?
Sí
Fin
238

FIG. 2b

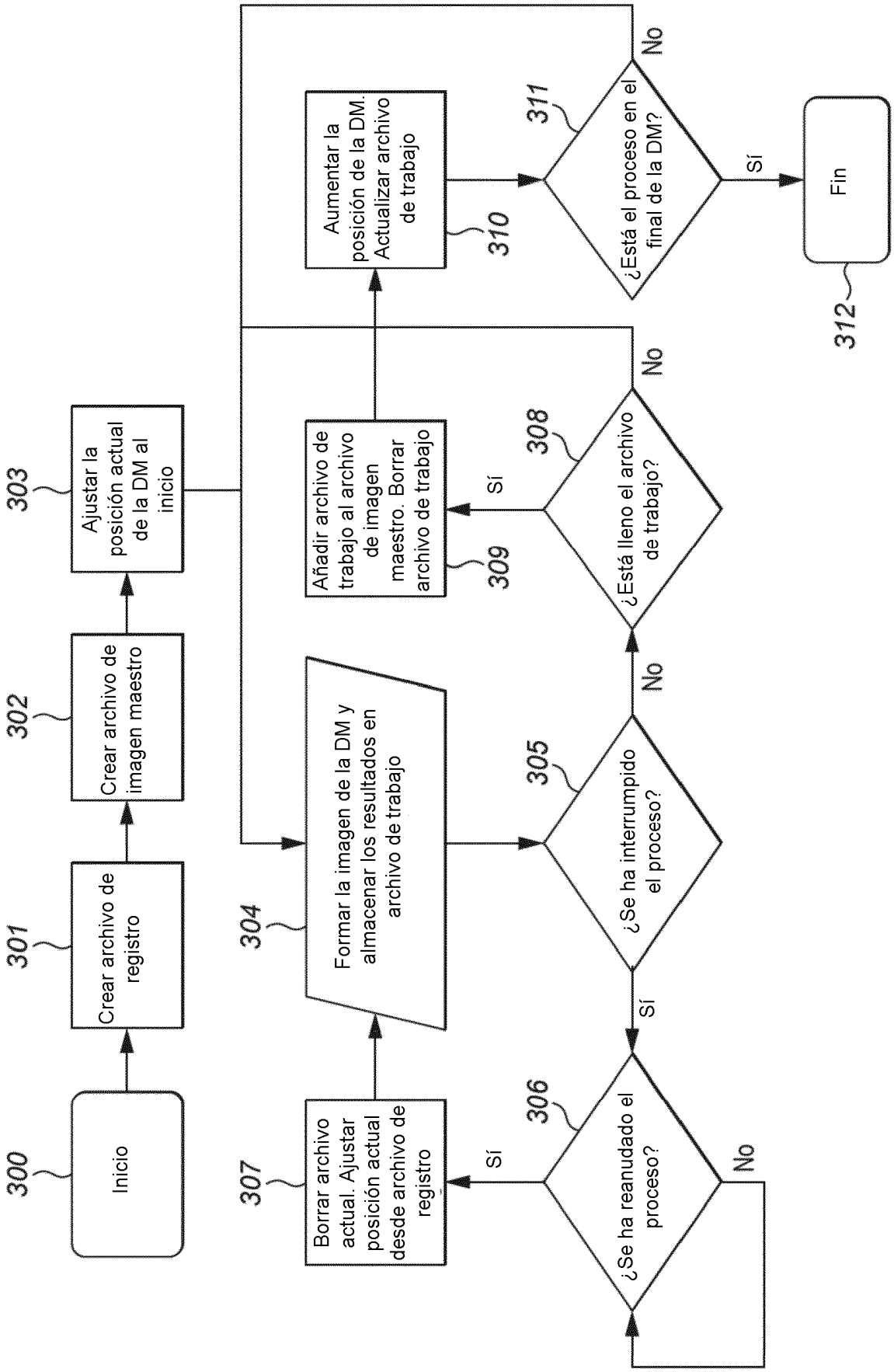
300
Inicio
301
Crear archivo de registro
302
Crear archivo de imagen maestro
303
Ajustar la posición actual de la DM al inicio
304
Formar la imagen de la DM y almacenar los resultados en archivo de trabajo
305
¿Se ha interrumpido el proceso?
306
¿Se ha reanudado el proceso?
307
Borrar archivo actual. Ajustar posición actual desde archivo de registro
308
¿Está lleno el archivo de trabajo?
309
Añadir archivo de trabajo al archivo de imagen maestro. Borrar archivo de trabajo
310
Aumentar la posición de la DM. Actualizar archivo de trabajo
311
¿Está el proceso en el final de la DM?
312
Fin
Sí
No

FIG. 3

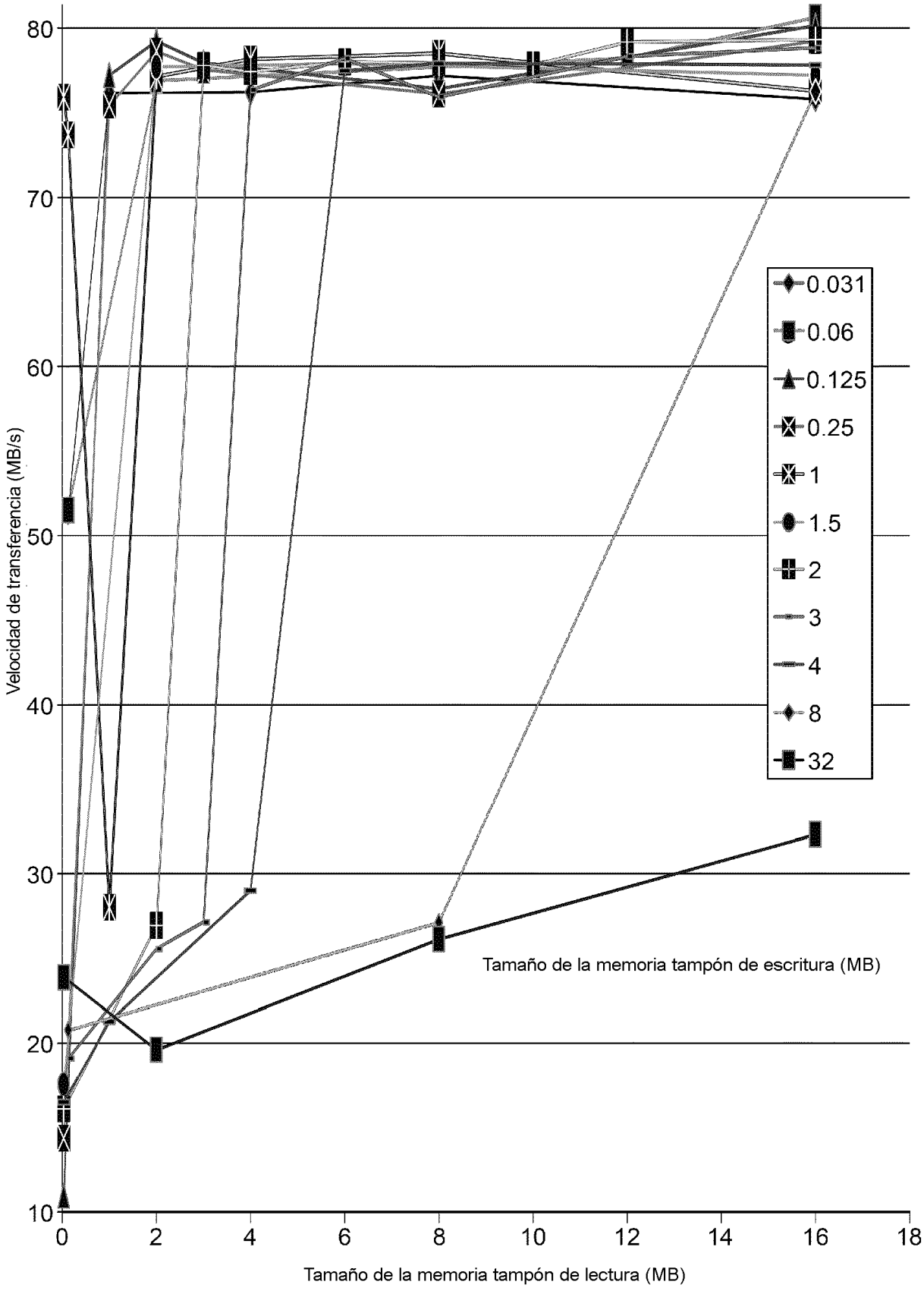
80
70
60
50
40
30
20
10
Velocidad de transferencia (MB/s)
0
2
4
6
8
10
12
14
16
18
Tamaño de la memoria tampón de lectura (MB)
Tamaño de la memoria tampón de escritura (MB)
0.031
0.06
0.125
0.25
1
1.5
2
3
4
8
32

FIG. 4