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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 September 2021 (23.09.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/188604 A1

(51) International Patent Classification:
G06F 21/50 (2013.01) *G06F 16/25* (2019.01)
G06F 21/62 (2013.01) *G06F 16/28* (2019.01)
G06F 16/21 (2019.01)

(21) International Application Number:
PCT/US2021/022646

(22) International Filing Date:
17 March 2021 (17.03.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/990,880 17 March 2020 (17.03.2020) US

(71) Applicant: **CENTERBOARD, LLC** [US/US]; 2601 Wendler Court, Wake Forest, NC 27587 (US).

(72) Inventors: **RENN, Donna**; 135 Deerfield Farms Road, Norlina, NC 27563 (US). **GIBBS, Lawrence Franklin**; 2601 Wendler Court, Wake Forest, NC 27587 (US).

(74) Agent: **HOBSON, Alex**; P.O. Box 21055, Sedona, AZ 86351 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, ST, 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, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

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

(54) **Title:** DIGITAL FILE FORENSIC ACCOUNTING AND MANAGEMENT SYSTEM

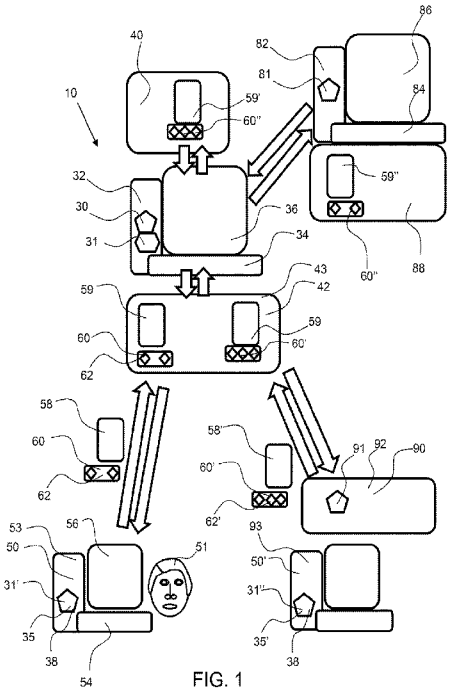


FIG. 1

(57) **Abstract:** A digital file forensic accounting and management system collects forensic data for a digital file that is stored and accounted for in a datastore. The digital files and the associated forensic data may be retrieved from the datastore by a third party to verify the authenticity of the digital file. An interface program is utilized to collect forensic data about a file upon creation of the file and/or when the file is transferred to the datastore. An interface program may be a framework that is operated on a file producing program that a file provider used to create a digital file. An interface program may be an origination driver that is operated on the file providing computer. An interface program may be a directory monitoring program that transfers the digital file and forensic data to the datastore upon saving the file to the monitored directory.

WO 2021/188604 A1

DIGITAL FILE FORENSIC ACCOUNTING AND MANAGEMENT SYSTEM

Cross Reference To Related Applications

[0001] This application claims the benefit of priority to U.S. provisional patent application No. 62/990,880, filed on March 17, 2020; the entirety of which is hereby incorporated by reference herein.

BACKGROUND OF THE INVENTION

Field of the Invention

[0002] The invention relates a digital file forensic accounting and management system that acquires forensic data for digital files and provides a database for said files for retrieval and accounting.

Background

[0003] There are a wide array of circumstances where a digital file is required and proof of authenticity of the file is desired or required. Unfortunately, a file provider can, in many circumstances, modify a file that they are providing for certification. A file receiver may simply trust that a digital file is authentic and unaltered. For example, a software provider may have to certify that they are Payment Card Industry ("PCI") compliant before providing the software to a customer. The software provider may have to provide proof that they are PCI compliant, such as providing a copy of a software assessment or proofs or artifacts including proof of insurance and proof of vulnerabilities. The documents provided by the assessment companies are sent to the software provider and are then typically provided by the software provider to their potential customer. The software provider may alter the finding of the assessment or certification before providing the report to the customer. This practice can put the customer at risk and leave them liable for damages resulting from utilizing the software providers software.

SUMMARY OF THE INVENTION

[0004] The invention is directed to a proactive digital file forensic accounting and management system that proactively and dynamically collects forensic data for a digital file that is stored and accounted for in a datastore. The collection of the forensic data for the associated digital file at the time of creation of the digital file improves the efficiency of the forensic accounting system and computing system by ensuring the data is authentic as the creation of the file is controlled through the proactive digital file forensic accounting and

management system. This provides for a more reliable system that people and companies can entrust for receiving authentic digital files. The digital files and the associated forensic data may be retrieved from the datastore to verify the authenticity of the digital file. For example, a software provider may be required to certify that they are PCI compliant before a new customer will purchase or license the software from the software provider. The software provider may employ a PCI auditor to provide PCI compliance certifications to the new customer. The PCI auditor may have a framework provided by the exemplary digital file forensic accounting and management system that collects forensic data about the PCI compliance digital file and this digital file and associated forensic data may be transferred to a datastore. This file package, the digital file and forensic data, may be encrypted with an encryption program prior to the file package being transferred to the datastore. The potential new customer may receive the PCI compliance document and associated forensic data from the datastore and be sure that the digital file is authentic and not altered in anyway. An exemplary digital file forensic accounting and management system may also use an origination driver that is operated by a file providing computer to collect forensic data about a digital file. The origination driver may be used in the transfer of the digital file and forensic data to the datastore. An exemplary digital file forensic accounting and management system may utilize a directory monitoring program that collects forensic data about a digital file when it saved into a monitored directory. The directory monitoring program then sends the collected forensic data upon creation of the digital file to the datastore along with a chain of custody for the digital file.

[0005] The digital files and forensic data associated with the digital file, a file package, may be retrieved from a datastore but may not be altered within the datastore. A system computer may track any retrieval of a digital file or file package from the datastore for future review. A record of access to a digital file may be part of a chain of custody recorded by the digital file forensic accounting and management system.

[0006] An exemplary digital file forensic accounting and management system utilizes an interface program to collect forensic data regarding a digital file that is provided to a datastore. An interface program may be a framework that is operated on a file providing computer or operated by a file producing program. A framework may be code that is licensed by a file producing program company, such as an accounting company, a records company, a compliance company and the like. This code or Application Program Interface (API) may be integrated into their own software program or file producing program, to provide the required functions of the digital file forensic accounting and management system. The code may include libraries and encryption program or software for encrypting the digital file before

transfer to the datastore. A file provider may have to provide a file to third party and may use the file producing program to produce the file. Upon creating the file, the framework may then collect the forensic data and transfer the file along with the forensic data to a datastore. A third party may then retrieve the file package from the datastore including the digital file and the forensic data. A framework may utilize an origination driver to transfer the file package to the datastore and a framework may utilize an encryption program, software or code to encrypt the digital file and/or forensic data before transfer to the datastore.

[0007] An exemplary digital file forensic accounting and management system utilizes an interface program to collect forensic data regarding a digital file that is provided to a datastore. An interface program may be an origination driver that is operated on a file providing computer. The origination driver may have software to send a digital file and forensic data to the datastore, and may operate like a print driver, wherein the file provider prints using the origination driver to the datastore. When the digital file is transferred, the forensic data, such as the time, date, geolocation of origination, computer identification for producing the digital file and the like are transferred to the datastore. A third party may then retrieve the file package from the datastore including the digital file and the forensic data. An origination driver may utilize an encryption program, software or code to encrypt the digital file and/or forensic data before transfer to the datastore.

[0008] An exemplary digital file forensic accounting and management system utilizes an interface program to collect forensic data regarding a digital file that is provided to a datastore. An interface program may be a directory monitoring program that is operated on a file providing computer or within the cloud. The directory monitoring program may have software to send a digital file and forensic data to the datastore when the digital file is saved into a monitored directory. The directory monitoring program may not allow files to be opened from the monitored directory or modified in any way in the monitored directory. A file in a monitored directory may not be stored in the monitored directory and may be transferred to a datastore. A digital file saved in the monitored directory may be sent to a datastore for retrieval by a third party. Note the that the third party and the file provider may be part of the same company and the datastore may be the company's database or datastore. A directory monitoring program may utilize an encryption program, software or code to encrypt the digital file and/or forensic data before transfer to the datastore.

[0009] A datastore may be a database of a company that collects digital files for said company. A datastore may be part of a digital file forensic accounting and management system that is operated by a separate company from the file producing software or a file provider. An

exemplary digital file forensic accounting and management system may manage the datastore and keep records of any access to the digital files in the datastore. Each time a digital file is retrieved from the datastore, the digital file forensic accounting and management system, utilizing a system program, may keep a record, including retrieval forensic data of the transfer of the digital file. This retrieval forensic data may include data about the digital package provided and information about the requestor, such as any of the forensic data defined herein including, date and time of retrieval, retrieving computer ID, retrieving geodata or location of retrieving computer, etc. Also, retrieved data may be encrypted before being transferred to a third party and may utilize an encryption program, software or code to encrypt the digital file and/or forensic data before transfer to the third party.

[0010] An exemplary digital file forensic accounting and management system may include a virtual machine for interface by a file providing computer. A virtual machine may include a virtual machine website that a file producing computer access to provide a digital file to the datastore. The system computer of the digital file forensic accounting and management system may operate the virtual machine or be linked with the virtual machine.

[0011] In an exemplary embodiment, a file producing computer logs into or otherwise access the virtual machine, such the virtual machine website, to provide a digital file directly from the file providing computer. Again, the file providing computer may run an interface program to enable forensic data to be collected and submitted along with the digital file.

[0012] In another embodiment, the file producing computer access a file origination computer through the virtual machine. A file provider may access the virtual machine website and then access a file origination website through the virtual machine. The virtual machine may have links for the file provider to access file origination websites. The file provider may have to log into the virtual machine and may also have to log into the file origination website before creating a digital file through the file origination interface and website. The digital file and associated forensic data may be transferred directly from the file origination computer or file origination database to the datastore through the system computer.

[0013] A file producing computer may interface with a file origination computer through a file origination website. The file origination computer may operate an interface program to enable a digital file and associated forensic data to be transferred directly to the system computer from the file origination computer. A file provider may access the file origination website through their file providing computer and produce a digital file through the file origination website. The file origination website and computer may license the interface program to allow for direct transfer to the datastore.

[0014] An exemplary file producing computer may be a mobile device, such as a mobile phone and an interface program may be an App that operates on the mobile device. The interface program may include a print driver to enable forensic data about a scan produced by the mobile device to be provided along with the scan, or digital file, to the datastore. A mobile device may use a camera of the mobile device to produce a scan of a file to produce the digital file.

Benefits of The Digital File Forensic Accounting And Management System

[0015] An exemplary digital file forensic accounting and management system addresses data integrity, data recovery, data location and imaging. This is done by interfacing with a file producing computer or file providing computer through an interface program to collect the associated forensic data at the time of creation of the digital file versus after an incident which would require multiple tools and a disk image. This proactive collection of forensic data at the time of file creation ensures integrity of the file and authenticity of the forensic data. This enables a new means of collecting forensic data and improves the efficiency of the computing system for this purpose.

[0016] An exemplary digital file forensic accounting and management system controls digital files in a datastore and allows third parties to retrieve the digital file and forensic data but these third parties are not allowed to modify these files in any way. An access log may be kept for all parties given access to the digital file and forensic data. This is a dynamic chain of custody for the lifetime of the file. In traditional forensics, this would only start after legal seizure of a disk and an investigation begins. Our product preserves the file with the forensics data at the point of creation and maintains that chain of custody forever. There are no gaps.

[0017] Management of the digital file in a controlled datastore by a system computer improves issues relating to obfuscation, data hiding and malware designed to prevent or mislead forensic analysis. Since the forensics are gathered and stored up front, there is no chance for someone to tamper or change and forensic data.

[0018] Incident first responders: Verifying the trustworthiness of cloud providers, response time and reconstruction. An exemplary digital file forensic accounting and management system verifies the trustworthiness of cloud providers, response time and reconstruction as the interface program is licensed to specific file producers that may be cloud based with respect to file provider interface. If forensics is needed and the data is located on a cloud provider, legal action must be taken against the file owner and the cloud provider. The cloud provider is forced

to turn over other client's files that may be on the same disk they would have to image and will be hesitant to turn that information over. This results in a lot of privacy issue.

Definitions:

[0019] Forensic data, as used herein includes, but is not limited to, metadata including document metadata, time and date data, such as time and date of origination or document creation, modification date, geolocation data including location of creation and modification, origination software data or the software used to create digital file, created by data, application name, document title, author of the document, identified user creating the file, couple keywords, word count, character count, character count with spaces, file size, number of pages, computer data, such as computer ID or computer name, computer owner, logged in ID, operating system forensics, application data forensics, path, owner, group(unix) file permissions on operating system (OS), address of computer, MD5 Hash, SHA-1 Hash, SHA-256 Hash, file signature, and the like.

[0020] A computer, as used herein, is a computing device that can create directly or interface with a file producing program to create a digital file and includes a personal computer, laptop, mobile device including a tablet computer or mobile phone.

[0021] Data collection involves identification and preservation as well as collecting, analyzing, and reporting data.

[0022] Electronic discovery utilizes all those processes and generally collects active data.

[0023] Active data is classified as information and data that is easily available through file storage and program managers utilized by a business or individual.

[0024] A forensic analysis of data is needed when the litigation requires a deeper look at the data. A digital forensic specialist sorts through data in search of hidden files or deleted data to help provide more-reliable evidence.

[0025] Data being stored automatically. After many years of digital backups, automatically stored data may have been removed from a server. Forensics can discover this data typically located on a hard drive.

[0026] Deleted data. Any files that have been deleted from the system will usually remain on the computer's hard drive. Forensics will be used to locate this information as long as the hard drive has not been overwritten or wiped.

[0027] Wiping software. Most computer forensic specialists can determine if any hard drive wiping software was used on a computer. This can help make a case that data was destroyed purposely.

[0028] Framework, as used herein, is software that enables the functions and procedures allowing the integration of software applications into a larger software package. Framework may include Application Program Interface (API), code libraries and other programs.

[0029] Payment Card Industry (PCI), as used herein, is an industry standard designed to make it safer to use credit cards online by making sure that business collecting credit card data transmit and store it securely.

[0030] A virtual machine is accessed through the internet by a file provider and may include a website that the file provider interfaces with, a system computer that operates a system software program. A file provider may have to log into the virtual machine using a login and password and the virtual machine may obtain forensic data regarding the file provider including location information, computer origination information and the like. A virtual machine may utilize an interface program that operates on the system computer, the file providing computer and/or on a file origination computer and/or file origination database.

Example 1: PCI Compliance

[0031] A software provider is in negotiations with a new potential customer. The software provide has been requested to provide proof of PCI compliance. An exemplary digital file forensic accounting and management system may be used to provide certified PCI compliance data to the new potential customer. A PCI compliance company may have compliance software that includes a framework provided by the digital file forensic accounting and management system. The software provider may utilize the PCI compliance software that collects forensic data about a PCI compliance digital file. The PCI compliance digital file may include software assessment or proofs or artifacts including proof of insurance and proof of vulnerabilities. This PCI compliance digital file and associated forensic data may then be send to a datastore and subsequently retrieved by the potential new customer. The new customer can then be sure that the assessment and certifications are authentic.

Example 2: Loan Approval

[0032] A new home buyer is seeking loan approval. They are working with a bank to secure a loan for the new home. The bank may require the home buyer to transfers one or more files to the bank's datastore via an origination driver. The origination driver may be provided to the home buyer's computer, such as being downloaded from the bank's website. The home buyer may then use the origination driver to provide digital file documents for the loan application, such as pay stubs, saving documents, credit reports and the like. The origination driver collects forensic data about the digital files.

Example 3: Intellectual Property

[0033] A company may have a new invention submission program for their employees. The employee may use a directory monitoring program to collect data about invention submission saved into a monitored directory. These new invention digital files may be transferred to a datastore, along with forensic data about the new invention digital file. This forensic data may be used to provide evidence and certification of the creator of the digital file and time of creation. This forensic data may be used to settle disputes regarding who was the first to invent.

Example 4: Records

[0034] A public records system collects and makes public record documents available to third parties. The public records system utilizes a datastore for the public records. Third parties can receive a copy of a digital file package, digital file and forensic data, upon request an upon paying a fee. The public records system uses an interface program, such as a framework, origination driver or directory monitoring program to transfer public records into the datastore.

[0035] The summary of the invention is provided as a general introduction to some of the embodiments of the invention, and is not intended to be limiting. Additional example embodiments including variations and alternative configurations of the invention are provided herein.

BRIEF DESCRIPTION OF SEVERAL VIEWS OF THE DRAWINGS

[0036] The accompanying drawings are included to provide a further understanding of the invention and are incorporated in and constitute a part of this specification, illustrate embodiments of the invention, and together with the description serve to explain the principles of the invention.

[0037] Figure 1 shows a diagram of an exemplary digital file forensic accounting and management system that collects and stores digital files and associated forensic data that can be transferred to a third-party computer.

[0038] Figure 2 shows a diagram of an exemplary digital file forensic accounting and management system wherein an interface program running on a file producing program collects forensic data when created in the file producing program by a file providing computer and wherein the forensic data is transferred to the system datastore along with the digital file by the file producing program.

[0039] Figure 3 shows a diagram of an exemplary digital file forensic accounting and management system wherein an interface program running on a file producing computer collects forensic data when created in the file producing program by a file providing computer and wherein the forensic data is transferred to the system datastore along with the digital file by the file providing computer.

[0040] Figure 4 shows a diagram of an exemplary digital file forensic accounting and management system wherein a directory monitoring interface program running on a file providing computer collects forensic data when a file in the directory is saved to the monitored directory. A file may not be allowed to be opened and manipulated within the directory. In an exemplary embodiment, a file saved in the monitored directory is transferred to a datastore.

[0041] Figure 5 shows a flowchart of an exemplary method utilized by a digital file forensic accounting and management system to collect a digital file and forensic data for said digital file using a framework that is operated by a file producing program.

[0042] Figure 6 shows a flowchart of an exemplary method utilized by a digital file forensic accounting and management system to collect a digital file and forensic data for said digital file using an origination driver that is operated by a file providing computer.

[0043] Figure 7 shows a flowchart of an exemplary method utilized by a digital file forensic accounting and management system to collect a digital file and forensic data for said digital file using a directory monitoring program that is operated by a file providing computer.

[0044] Figure 8 shows a flowchart of an exemplary method utilized by a digital file forensic accounting and management system to collect a digital file and forensic data for said digital file using a virtual machine that a file provider uses to interface with a file origination interface, such as a website to produce a digital file.

[0045] Corresponding reference characters indicate corresponding parts throughout the several views of the figures. The figures represent an illustration of some of the embodiments of the present invention and are not to be construed as limiting the scope of the invention in any manner. Further, the figures are not necessarily to scale, some features may be exaggerated to show details of particular components. Therefore, specific structural and functional details disclosed herein are not to be interpreted as limiting, but merely as a representative basis for teaching one skilled in the art to variously employ the present invention.

DETAILED DESCRIPTION OF THE ILLUSTRATED EMBODIMENTS

[0046] As used herein, the terms "comprises," "comprising," "includes," "including," "has," "having" or any other variation thereof, are intended to cover a non-exclusive inclusion. For example, a process, method, article, or apparatus that comprises a list of elements is not necessarily limited to only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. Also, use of "a" or "an" are employed to describe elements and components described herein. This is done merely for convenience and to give a general sense of the scope of the invention. This description should be read to include one or at least one and the singular also includes the plural unless it is obvious that it is meant otherwise.

[0047] Certain exemplary embodiments of the present invention are described herein and are illustrated in the accompanying figures. The embodiments described are only for purposes of illustrating the present invention and should not be interpreted as limiting the scope of the invention. Other embodiments of the invention, and certain modifications, combinations and improvements of the described embodiments, will occur to those skilled in the art and all such alternate embodiments, combinations, modifications, improvements are within the scope of the present invention.

[0048] As shown in FIG. 1, an exemplary digital file forensic accounting and management system 10 utilizes an interface program 31 to collect forensic data 60 from a file provider 51. The interface program may be running on a virtual machine, wherein a user interfaces with the virtual machine 42 by interfacing with a virtual machine website 43, for example. The user may open or log into the virtual machine to prepare a digital file 58, with the associated forensic data 60, to a database 40. An interface program 31 may be operated through the virtual machine and/or an interface program 31', or portion thereof, may be transferred to a file providing computer 50 and operate on said file providing computer to collect forensic data about a digital file 58, that is transferred to the datastore 40. A file provider 51 may use the file providing interface 54 and display 56 of the file providing computer 50 to create a file and send a digital file to the datastore through the virtual machine 42. The interface program 31 may be an origination driver 38 and a file providing user may use the origination driver to print the document to the system computer 32 or datastore 40. The forensic data may include the date and time of creation of the digital file, geodata, software creation data, certificates and the like. A system program 30 and/or a third-party interface program 81 may be used by a third-party computer 82 to obtain a verified digital file 59 and associated forensic data 60 from the datastore. An origination driver may utilize an encryption program 35, software or code to encrypt the digital file and/or forensic data before transfer to the datastore.

[0049] The virtual machine 42 may be configured to allow a file provider 51 to interface with a file origination interface 91, such as a file origination website 92 that create a digital file 58' that may include information from a file origination database 90. The digital file 58' and associated forensic data 60', may be transferred directly from the file origination website 92 or file origination computer 93 to the virtual machine 42 and datastore 40 to produce a verified digital file 59 having associated forensic data 60'. The file provider may input login credentials to the file origination interface 91 through the virtual machine such that the forensic data may include the file providing computer 50 information as well as the file origination interface 91, such as the file origination website 92 and/or file origination computer 93 forensic data.

[0050] The system computer 32 may receive the verified digital file 59 and directly deposit the verified digital file 59' to the datastore.

[0051] A third-party user may use a third party system interface 84 and display 86 of the third party computer 82 to obtain a verified digital file 59'' from the datastore. A third party may interface with the system computer 32 via the virtual machine 42 through a virtual machine website 43. The third-party computing system may interface with a third party database 88 to store verified digital files 59''and forensic data 60'' for said digital files. A system user may use the system interface 34 and display 36 of the system computer 32 to manage digital files within the datastore. In an exemplary embodiment, when the digital file is shared with a third party computer 82, permission from the file provider 51 may be required before the third party is given access to the verified digital file 59'' from the data store 40. The third party may be allowed to print or download the files, but may not be given access to the file owner to access them inside the datastore. The third party may be allowed to print or download the digital file but they may not be provided the metadata or allowed to modify the original digital file in the datastore. A chain of custody of the digital file may be kept in association with the digital file in the datastore. This chain of custody may include forensic data of any third party access, download, or print of the digital file and may include metadata regarding the third party, date, time, geographical location and the like.

[0052] As shown in FIG. 1, an exemplary digital file forensic accounting and management system 10 collects and stores verified digital files 59, 59' and associated forensic data 60, 60' from a plurality of file providing computers 50, 50', respectively. The file providing computers may operate an interface program 31, 31' to collect forensic data, such as metadata 62, 62' that is transferred to the datastore 40 as a verified digital file 59' and associated forensic data 60''. The forensic data may be collected as the file is create, such as when the interface software is a

framework software. Again, a third party computer 82 may interface with the system computer 32 to obtain a verified digital file 59'' and associated forensic data 60'', which may be stored in a third party database 88.

[0053] As shown in FIG. 1, the file providing computer 50 may be a mobile device 53, such as a smart phone. The smart phone may interface with the system computer 32 through a virtual machine 42 such as the virtual machine website 43. An interface program 31'may be an App that operates on the mobile device and may have a feature to enable a scan to create a digital file 58. The App may have drivers to enable forensic data 60 to be collected. The scan may include taking a picture via the mobile device or mobile phone.

[0054] As shown in FIG. 2, an exemplary digital file forensic accounting and management system 10 utilizes an interface program 31' running on a file producing program 70 to collect forensic data 60' about a digital file 58, such as when the file is created in the file producing program by a file providing computer 50. In an exemplary embodiment, a file origination interface 91 may have software that enables a file provider 51 to request that a digital file be transferred directly to the datastore 40. A file origination interface may include a file origination website 92 and interface that provides an option to the file provider 51, to transfer a digital file 58 to the datastore 40. A file provider may interface directly with the file producing program 70 having the file origination interface 91 that operates an interface program 31'. The file origination interface, such as an accounting software company, may subscribe to or have a license from the digital file forensic accounting and management system 10 to enable this direct submission of a digital file 58 and forensic data 60' directly to a datastore 40, for a file provider. The forensic data is transferred to the system datastore 40 along with the digital file 58 by the file producing program 70. For example, a file provider 51 may use the file providing interface 54 of the file providing computer 50 to interface with the file providing program 70, such as an accounting software, that the file providing user logs into to provide data to create a digital file. The file providing user may interface directly with the file providing program or through a virtual machine 42 as shown in FIG. 1. The accounting software, or file producing program, may run the interface program 31', such as a framework 39 while the digital file is created or when the digital file is saved and/or transferred to the datastore 40. The accounting software company may license the interface program or framework to enable the forensic data to be provided with digital files to the datastore. Note that the interface program may be running on a file origination interface 91, through a file origination website 92, wherein data from a file origination database 92 is utilized to create the digital file 58 that is transferred from the file origination interface to the datastore 40 and which

may include forensic data 60 about the file providing computer 50 as well as forensic data 60' about the file origination interface 91. Again, a third party computer 82 may interface with the system computer 32 to obtain a verified digital file 59' and associated forensic data 60', which may be stored in a third party database 88. A framework 39 may utilize an encryption program 35, software or code, to encrypt the digital file and/or forensic data before transfer to the datastore. The framework may operate at least in part on the file origination computer 93 or may be accessed by the file origination computer through the virtual machine.

[0055] As shown in FIG. 3, an exemplary digital file forensic accounting and management system 10 utilizes an interface program 31' running on a file producing program 70 to collect forensic data 60 about a digital file 58, such as when the file is created in the file producing program by a file providing computer 50. This forensic data 60 is transferred to the system datastore 40 along with the digital file 58 by the file providing computer 50. For example, a file providing user may use the file providing interface 54 of the file providing computer 50 to interface with the file providing program 70, such as an accounting software, that the file providing user logs into to create a digital file. The accounting software, or file producing program, may run the interface program 31' while the file is created or when the file is saved and/or transferred, such as to the datastore 40, or directly to a third party. In this embodiment, the digital file and associated forensic data may be transferred to the file providing computer 50 before being sent via the file providing computer using interface program 31'', such as an origination driver 38, to the datastore. The file producing computer may also run the interface program 31' or a portion thereof. The file producing program 70, such as an accounting software that may be accessible through the internet via a website, may license the interface program 31' from the digital file forensic accounting and management system 10.

[0056] As shown in FIG. 4, an exemplary digital file forensic accounting and management system 10 utilizes an interface program 31' to transfer a digital file to datastore 40. The interface program is a directory monitoring interface program 37 that is transferred to the file providing computer 50. As shown, a directory monitoring interface program 37 may operate on the system computer 32 and a directory monitoring interface program 37' may operate on the file providing computer 50 to monitor a directory 52 of the file providing computer. The directory monitoring program runs on the file providing computer to collect forensic data 60 when a file is saved to the monitored directory. A digital file 58 saved to the monitored directory may be automatically transferred to the datastore 40 each time a digital file in saved to the directory. Again, a third-party computer 82 may access the datastore to obtain a verified digital file 59 and forensic data 60 which may be stored in a third-party database 88 as a

verified digital file 59' and verified forensic data 69'. A directory monitoring interface program 37 may utilize an encryption program 35, software or code to encrypt the digital file and/or forensic data before transfer to the datastore.

[0057] As shown in FIG. 5, an exemplary method of a digital file forensic accounting and management system uses a framework or API that is operated by a file producing program to collect a digital file and forensic data for said digital file. The framework is provided to a file producing program and may be licensed by the file producing program. A file provider may interface with the file producing program, such as an accounting program, to create a digital file and the framework may collect forensic data for this created digital file. The digital file and forensic data may then be transferred to a system computer and datastore for retrieval by a third party, such as an accountant. The file provider may view the digital file and/or forensic data but may not be able to alter it in any way after created. For example, a business owner may utilize an accounting program, the file producing program, to produce a report by providing financial input to the system. A framework integrated with the file producing program may collect the forensic data with respect to the digital file. The digital file and forensic data may be transferred to the datastore and the business owner's accountant may retrieve the digital file and forensic data to prepare a tax return, for example.

[0058] As shown in FIG. 6, an exemplary method of a digital file forensic accounting and management system uses an origination driver that is operated by a file providing computer to collect a digital file and forensic data. A file provider may download an origination driver from a system computer or system database onto a file providing computer. The file provider may then produce a file and the origination driver may collect forensic data about the digital file that is transferred, along with the digital file, to a datastore. For example, an employee may have a new idea for an invention and may want to submit it to their employer. The employer may have an idea submission program that requires the employee to utilize the origination driver to submit the idea to the companies datastore. The forensic data may include the geodata, a time stamp and the like.

[0059] As shown in FIG. 7, an exemplary digital file forensic accounting and management system uses a directory monitoring program that is operated by a file providing computer to collect a digital file and forensic data. A file providing computer may receive a directory monitoring program, such as from a system computer, a system database or a file producing program. The file provider may produce a digital file and then save the file to a monitored directory. The directory monitoring program may collect forensic data about the digital file as it is saved to the monitored directory. The saved digital file and associated forensic data may

be transferred to a datastore. Each new digital file saved to the monitored directory, may be transferred to the datastore along with the associated forensic data. A file provider may not have access to the monitored directory except to save new files therein. Files in the monitored directory may not be allowed to be opened and modified by a file provider.

[0060] As shown in FIG. 8, an exemplary digital file forensic accounting and management system uses a virtual machine that a file provider interfaces with to produce a digital file via a file origination interface. An interface program may be running on a file origination interface through a file origination website, wherein data from a file origination database is utilized to create the digital file. The digital file is transferred from the file origination interface to the datastore along with forensic data about the file providing computer as well as forensic data about the file origination interface.

[0061] It will be apparent to those skilled in the art that various modifications, combinations and variations can be made in the present invention without departing from the scope of the invention. Specific embodiments, features and elements described herein may be modified, and/or combined in any suitable manner. Thus, it is intended that the present invention cover the modifications, combinations and variations of this invention provided they come within the scope of the appended claims and their equivalents.

What is claimed is:

1. A digital file forensic accounting and management system comprising:
    a) a file providing computer;
    b) an interface program;
    c) a datastore;
    wherein the interface program collects forensic data about a digital file and wherein said digital file and said forensic data are transferred to said datastore;
    wherein the forensic data includes origination data for said digital file.
2. The digital file forensic accounting and management system of claim 1, wherein the forensic data comprises metadata.
3. The digital file forensic accounting and management system of claim 1, wherein the forensic data comprises origination data that is associated with said file providing computer.
4. The digital file forensic accounting and management system of claim 1, wherein the forensic data comprises geodata that is associated with said geographical location of the file providing computer.
5. The digital file forensic accounting and management system of claim 1, wherein the interface program comprises an encryption program and wherein the digital file is encrypted when transferred to the datastore.
6. The digital file forensic accounting and management system of claim 1, wherein the interface program comprises an encryption program and wherein the digital file and the forensic data are encrypted when transferred to the datastore.
7. The digital file forensic accounting and management system of claim 1, wherein the interface program is configured and operated by the file providing computer to collect said forensic data for the digital file.
8. The digital file forensic accounting and management system of claim 1, further comprising a system computer and wherein the interface program is transferred to the file providing computer by said system computer and wherein said interface software program collects forensic data from said file providing computer.
9. The digital file forensic accounting and management system of claim 1, further comprising a file producing program, wherein the interface program is configured on and operated by said file producing program to collect said forensic data for the digital file.

10. The digital file forensic accounting and management system of claim 1, wherein the interface program is an origination driver.
11. The digital file forensic accounting and management system of claim 10, wherein the origination driver collects forensic data of the digital file, and wherein the digital file and forensic data are transferred to the datastore by said origination driver.
12. The digital file forensic accounting and management system of claim 1, wherein the interface program is a framework.
13. The digital file forensic accounting and management system of claim 12, wherein the framework collects forensic data of the digital file and wherein both the digital file and forensic data are transferred to the datastore.
14. The digital file forensic accounting and management system of claim 13, wherein the framework interfaces with the file providing computer and with a file software program to collect forensic data of the digital file.
15. The digital file forensic accounting and management system of claim 1, wherein the interface program is a directory monitoring software that monitors a monitored directory to collect forensic data for a digital file.
16. The digital file forensic accounting and management system of claim 15, wherein the monitored directory is on a file producing computer.
17. The digital file forensic accounting and management system of claim 15, wherein the directory monitoring software records digital file events of the monitored directory.
18. The digital file forensic accounting and management system of claim 17, wherein a digital file events includes a date and time of saving a digital file to the monitored directory.
19. The digital file forensic accounting and management system of claim 17, wherein a digital file events includes a date and time of retrieving a digital file in the monitored directory.
20. The digital file forensic accounting and management system of claim 1, wherein the interface program is transferred to a file producing program that the file providing computer uses to create a digital file within the file producing program; and

    wherein the digital file is transferred to the datastore through the file providing program.
21. The digital file forensic accounting and management system of claim 1, further comprising a virtual machine having a virtual machine website and wherein the file

providing computer interfaces with a virtual machine website to transfer the digital file and said forensic data to the datastore.

22. The digital file forensic accounting and management system of claim 1, further comprising:

a file origination computer;

wherein the file providing computer interfaces with said file origination computer to produce said digital file and said forensic data that is transferred to the datastore.

23. The digital file forensic accounting and management system of claim 22, wherein the digital file and the forensic data are transferred to the datastore from the file origination computer.

24. The digital file forensic accounting and management system of claim 22, wherein the digital file and the forensic data are transferred to the datastore from the file providing computer.

25. The digital file forensic accounting and management system of claim 22, wherein the file origination computer is accessed through a file origination website.

26. The digital file forensic accounting and management system of claim 25, wherein the file origination computer is accessed through a file origination website directly by the file providing computer.

27. The digital file forensic accounting and management system of claim 25, further comprising:

a virtual machine having a virtual machine website; and

wherein the file providing computer interfaces with said virtual machine website to interface with said file origination computer to produce said digital file and said forensic data to the datastore from the file origination computer.

28. The digital file forensic accounting and management system of claim 27, wherein the file providing computer accesses the file origination website through the virtual machine.

29. The digital file forensic accounting and management system of claim 1, wherein the file providing computer is a mobile device.

30. The digital file forensic accounting and management system of claim 29, wherein the mobile device is a mobile phone.

31. The digital file forensic accounting and management system of claim 29, wherein the interface program is a mobile App.

32. The digital file forensic accounting and management system of claim 31, wherein mobile App includes a print driver to collect forensic data about a scan produced by the mobile device.
33. The digital file forensic accounting and management system of claim 32, wherein the mobile device has a camera and wherein the camera is used to take a picture of a digital file.
34. The digital file forensic accounting and management system of claim 32, wherein the mobile device has a scanner and wherein the scanner is used to scan a digital file.
35. The digital file forensic accounting and management system of claim 34, where the scanner includes a camera of the mobile device.
36. A method of storing a digital file along with associated forensic data for the digital file comprising:
    a) providing a digital file forensic accounting and management system comprising:
        i) a file providing computer;
        ii) an interface program;
        iii) a datastore;
    b) utilizing the interface program to collect forensic data about said digital file;
    c) transferring said digital file and said forensic data to said datastore;

    wherein the forensic data includes origination data for said digital file.
37. The method of claim 36, wherein the forensic data comprises metadata.
38. The method of claim 36, wherein the forensic data comprises origination data that is associated with said file providing computer.
39. The method of claim 36, wherein the forensic data comprises geodata that is associated with said geographical location of the file providing computer.
40. The method of claim 36, wherein the interface program comprises an encryption program and wherein the digital file is encrypted when transferred to the datastore.
41. The method of claim 36, wherein the interface program comprises an encryption program and wherein the digital file and the forensic data are encrypted when transferred to the datastore.
42. The method of claim 36, wherein the interface program is configured on and operated by said file providing computer to collect said forensic data for the digital file.

43. The method of claim 36, further providing a system computer and wherein the interface program is transferred to the file providing computer by a system computer and wherein said interface software program collects forensic data from said file providing computer.
44. The method of claim 36, further providing a file producing program, wherein the interface program is configured on and operated by said file producing program to collect said forensic data for the digital file.
45. The method of claim 36, wherein the interface program is an origination driver.
46. The method of claim 45, wherein the origination driver collects forensic data of the digital file, and wherein the digital file and forensic data are transferred to the datastore by said origination driver.
47. The method of claim 36, wherein the interface program is a framework.
48. The method of claim 47, wherein the framework collects forensic data of the digital file and wherein both the digital file and forensic data are transferred to the datastore.
49. The method of claim 48, wherein the framework interfaces with the file providing computer and with a file software program to collect forensic data of the digital file.
50. The method of claim 36, wherein the interface program is a directory monitoring software that monitors a monitored directory to collect forensic data for a digital file.
51. The method of claim 50, wherein the monitored directory is on a file producing computer.
52. The method of claim 50, wherein the directory monitoring software records digital file events of the monitored directory.
53. The method of claim 52, wherein a digital file events includes a date and time of saving a digital file to the monitored directory.
54. The method of claim 52, wherein a digital file events includes a date and time of retrieving a digital file in the monitored directory.
55. The method of claim 36, wherein the interface program is transferred to a file producing program that the file providing computer uses to create a digital file within the file producing program; and

    wherein the digital file is transferred to the datastore through the file providing program.
56. The method of claim 36, further comprising a virtual machine having a virtual machine website and wherein the file providing computer interfaces with a virtual machine website to transfer the digital file and said forensic data to the datastore.
57. The method of claim 36, further comprising:

a file origination computer;

wherein the file providing computer interfaces with said file origination computer to produce said digital file and said forensic data that is transferred to the datastore.

58. The method of claim 57, wherein the digital file and the forensic data are transferred to the datastore from the file origination computer.

59. The method of claim 57, wherein the digital file and the forensic data are transferred to the datastore from the file providing computer.

60. The method of claim 57, wherein the file origination computer is accessed through a file origination website.

61. The method of claim 60, wherein the file origination computer is accessed through a file origination website directly by the file providing computer.

62. The method of claim 60, further comprising:

a virtual machine having a virtual machine website; and

wherein the file providing computer interfaces with said virtual machine website to interface with said file origination computer to produce said digital file and said forensic data to the datastore from the file origination computer.

63. The method of claim 62, wherein the file providing computer accesses the file origination website through the virtual machine.

64. The method of claim 36, wherein the file providing computer is a mobile device.

65. The method of claim 64, wherein the mobile device is a mobile phone.

66. The digital file forensic accounting and management system of claim 64, wherein the interface program is a mobile App.

67. The method of claim 66, wherein mobile App includes a print driver to collect forensic data about a scan produced by the mobile device.

68. The method of claim 67, wherein the mobile device has a camera and wherein the camera is used to take a picture of a digital file.

69. The method of claim 67, wherein the mobile device has a scanner and wherein the scanner is used to scan a digital file.

70. The method of claim 69, where the scanner includes a camera of the mobile device.

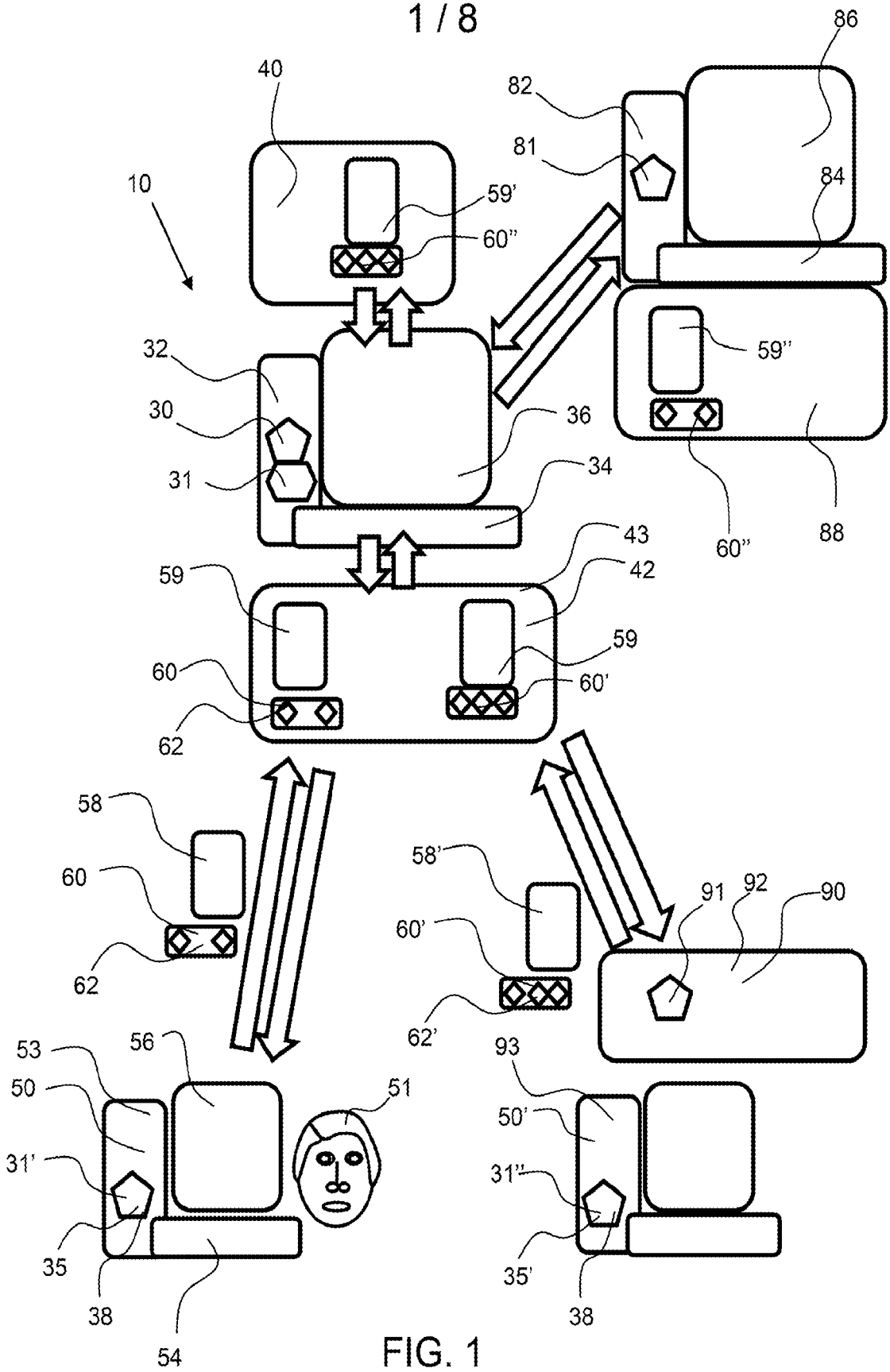

10
40
59'
60"
32
30
31
36
34
43
42
59
60
62
59
60'
58
60
62
58'
60'
62'
91
92
90
53
56
50
51
31'
35
38
54
93
50'
31"
35'
38
82
81
86
84
59"
60"
88

FIG. 1

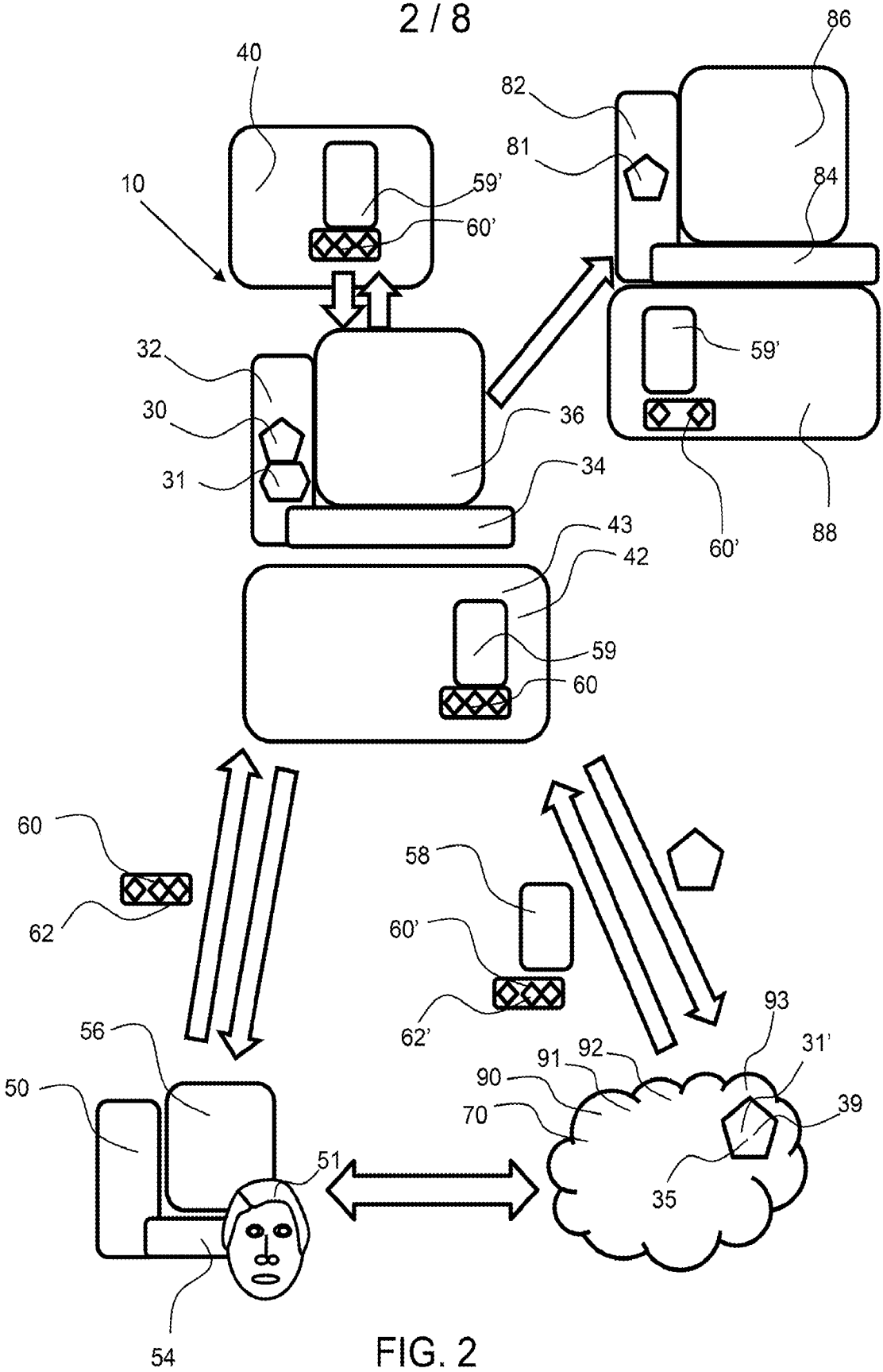

40
10
59'
60'
82
81
86
84
59'
88
60'
32
30
31
36
34
43
42
59
60
60
62
58
60'
62'
93
31'
92
91
90
70
39
35
56
50
51
54

FIG. 2

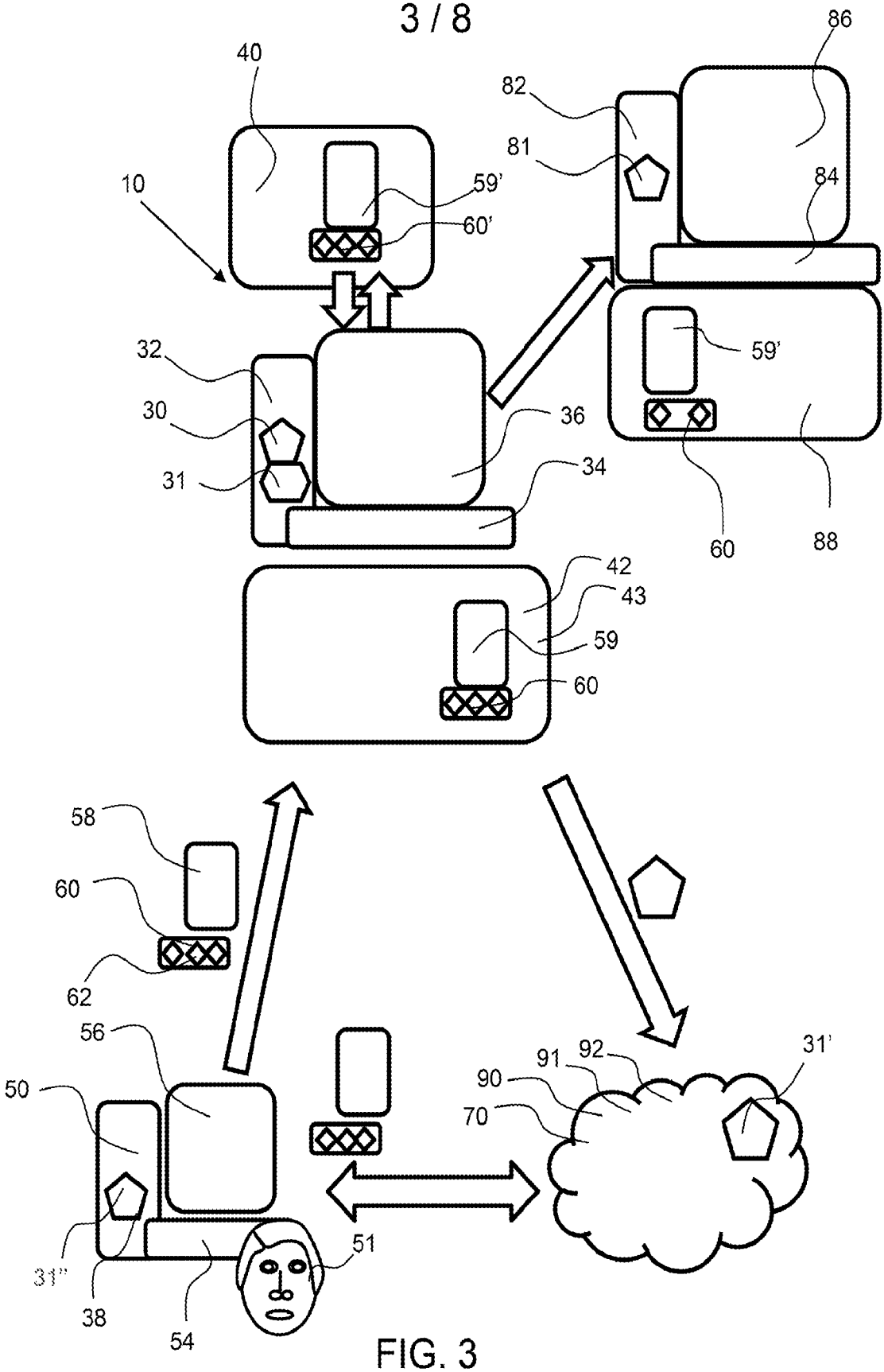

40
10
59'
60'
82
81
86
84
59'
32
30
31
36
34
60
88
42
43
59
60
58
60
62
56
50
31''
38
54
51
91
92
90
70
31'

FIG. 3

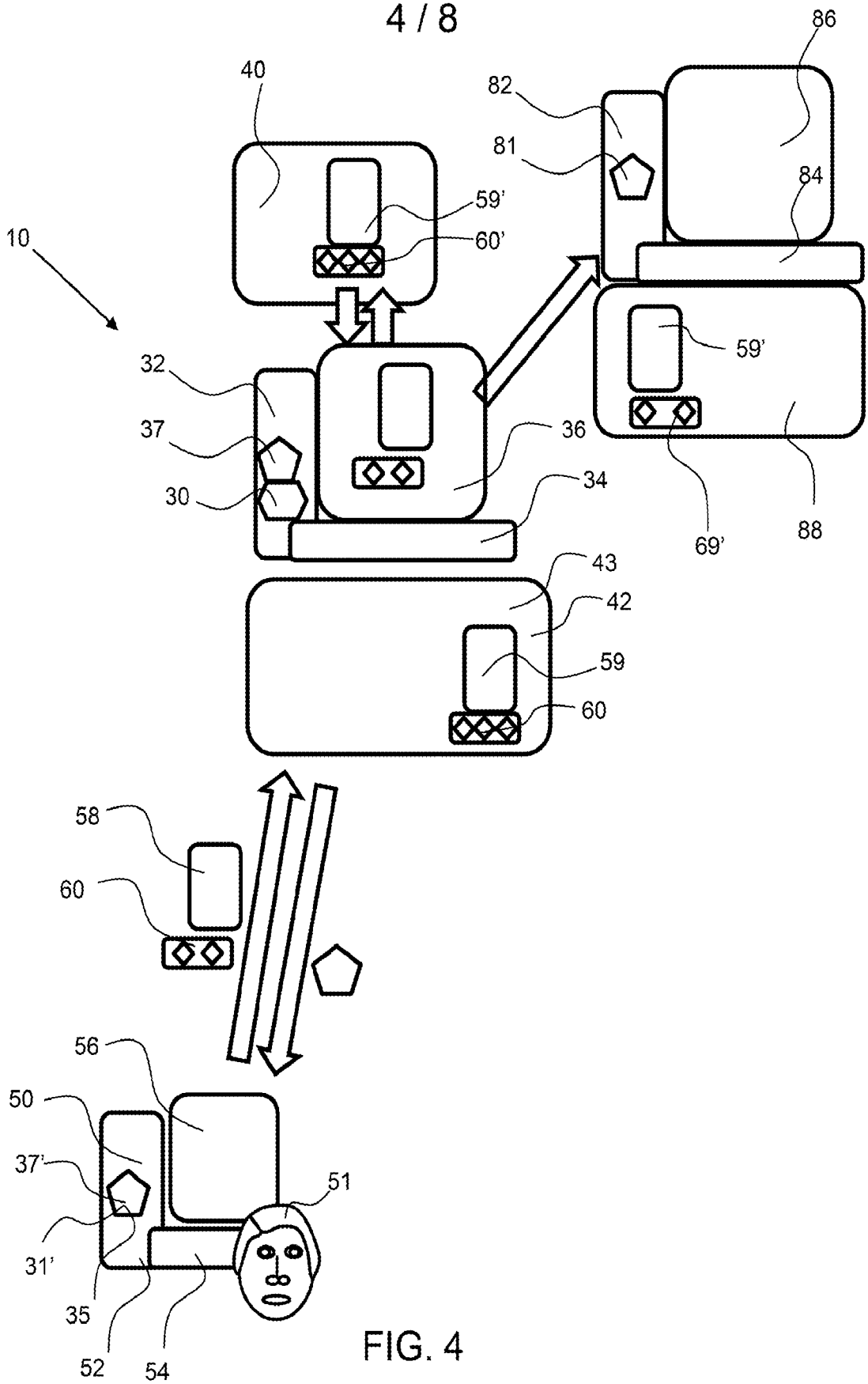

10
40
59'
60'
32
37
30
36
34
82
81
86
84
59'
69'
88
43
42
59
60
58
60
56
50
37'
31'
35
52
54
51

FIG. 4

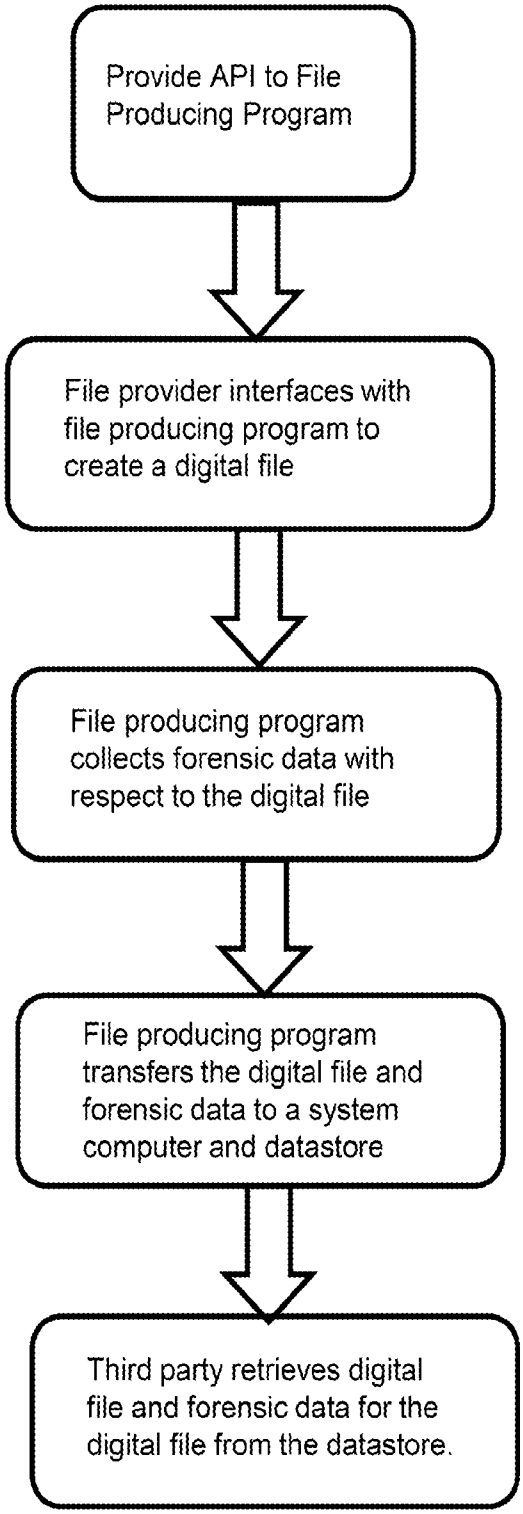

Provide API to File Producing Program
File provider interfaces with file producing program to create a digital file
File producing program collects forensic data with respect to the digital file
File producing program transfers the digital file and forensic data to a system computer and datastore
Third party retrieves digital file and forensic data for the digital file from the datastore.

FIG. 5

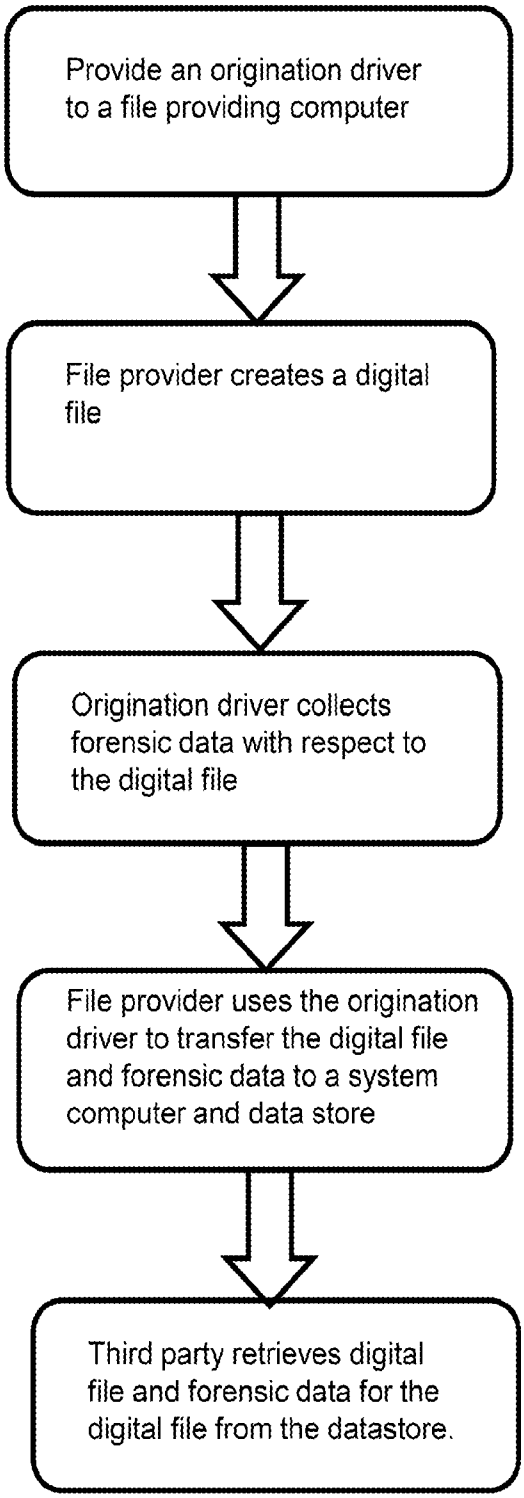

Provide an origination driver to a file providing computer
File provider creates a digital file
Origination driver collects forensic data with respect to the digital file
File provider uses the origination driver to transfer the digital file and forensic data to a system computer and data store
Third party retrieves digital file and forensic data for the digital file from the datastore.

FIG. 6

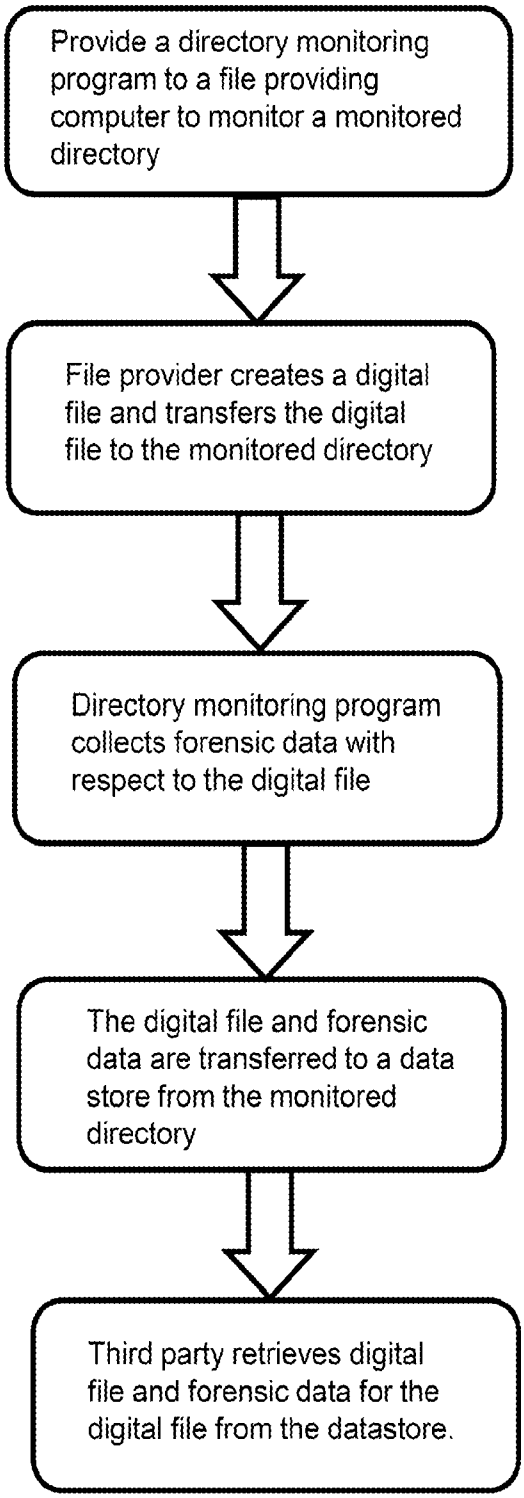

Provide a directory monitoring program to a file providing computer to monitor a monitored directory
File provider creates a digital file and transfers the digital file to the monitored directory
Directory monitoring program collects forensic data with respect to the digital file
The digital file and forensic data are transferred to a data store from the monitored directory
Third party retrieves digital file and forensic data for the digital file from the datastore.

FIG. 7

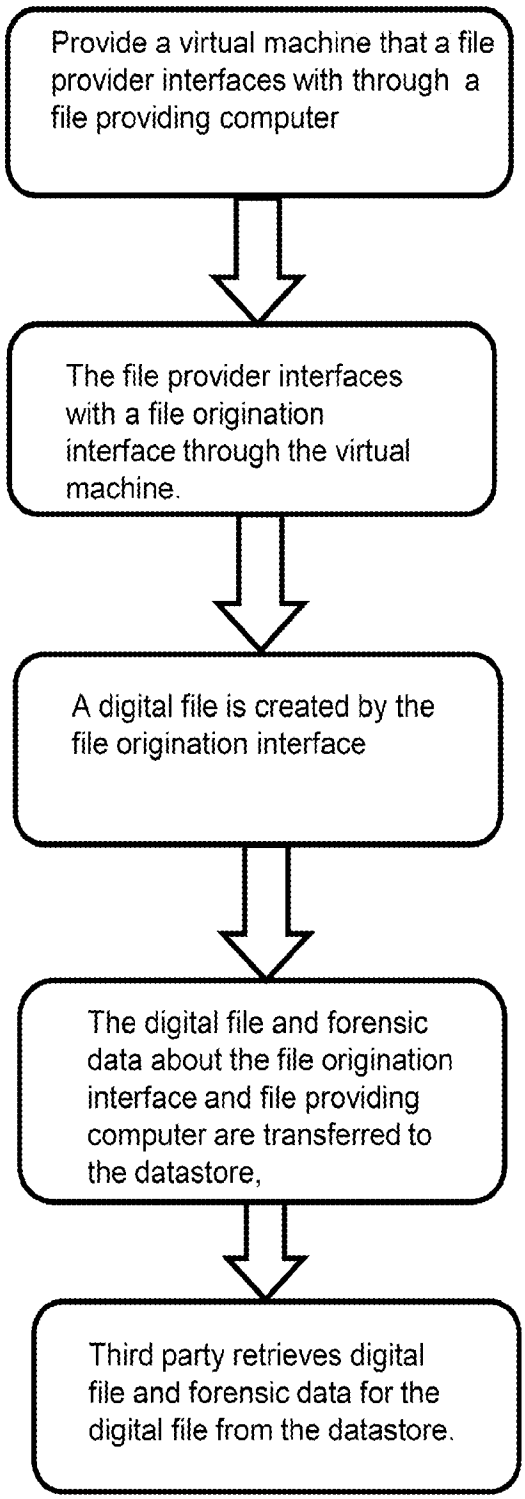

Provide a virtual machine that a file provider interfaces with through a file providing computer
The file provider interfaces with a file origination interface through the virtual machine.
A digital file is created by the file origination interface
The digital file and forensic data about the file origination interface and file providing computer are transferred to the datastore,
Third party retrieves digital file and forensic data for the digital file from the datastore.

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US21/22646

A. CLASSIFICATION OF SUBJECT MATTER

IPC - G06F 21/50; G06F 21/62; G06F 16/21; G06F 16/25; G06F 16/28 (2021.01)

CPC - G06F 21/62; G06F 16/25; G06F 21/50; G06Q 10/10; G06F 16/21; G06F 16/28

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)
See Search History document

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
See Search History document

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y --- A	US 2020/0042698 A1 (NATIONAL TECHNOLOGY & ENGINEERING SOLUTIONS OF SANDIA, LLC) 06 February 2020; abstract; paragraphs [0006], [0030], [0072]-[0079], [0086], [0121]; claim 4	1-4, 7-31, 36-39, 42-66 --- 5, 6, 40, 41 --- 32, 67
Y	US 2014/0181975 A1 (SPERNOW, W ET AL.) 26 June 2014; paragraphs [0014], [0016]	5, 6, 40, 41
A	US 2005/0259289 A1 (FERLITSCH, A ET AL.) 24 November 2005; entire document	1-70
A	WO 2020/046575 A1 (SOPHOS LIMITED) 05 March 2020; entire document	1-70

☐ 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
"D" document cited by the applicant in the international application
"E" earlier application or patent but 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
07 May 2021 (07.05.2021)	MAY 25 2021
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer Shane Thomas Telephone No. PCT Helpdesk: 571-272-4300