INTERFACE FOR MANAGING SPLITTABLE TIMESTAMPS ACROSS EVENT RECORDS

Applicant: SPLUNK INC., San Francisco, CA (US)

Inventors: R. David Carasso, San Rafael, CA (US); Micah James Delfino, San Francisco, CA (US)

Assignee: SPLUNK INC., San Francisco, CA (US)

Appl. No.: 13/747,177

Filed: Jan. 22, 2013

Publication Classification

Int. Cl. G06F 3/048 (2006.01)

U.S. Cl. CPC ...................................... G06F 3/048 (2013.01) USPC ...................................... 715/738

ABSTRACT

Embodiments are directed towards a graphical user interface to identify locations within event records with splittable timestamp information. A display of event records is provided using any of a variety of formats. A splittable timestamp selector allows a user to select one or more locations within event records as having time related information that may be split across the one or more locations, including, information based on date, time of day, day of the week, or other time information. Any of a plurality of mechanisms is used to associate the selected locations with the split timestamp information, including tags, labels, or header information within the event records. In other embodiments, a separate table, list, index, or the like may be generated that associates the selected locations with the split timestamp information. The split timestamp information may be used within extraction rules for selecting subsets of the event records.
Fig. 1
Fig. 2A
Fig. 2B
Fig. 3
Fig. 4
START

502 DISPLAY PLURALITY OF EVENT RECORDS

504 RECEIVE SPLITTABLE TIMESTAMP LOCATION SELECTIONS

506 ASSOCIATE LOCATION SELECTIONS WITH SPLITTABLE TIMESTAMPs

508 MORE SPLIT TIMESTAMPs?

510 RECEIVE EXTRACTION RULE USING SPLITTABLE TIMESTAMPS

512 EXTRACT EVENT RECORDS USING EXTRACTION RULE WITH SPLITTABLE TIMESTAMPS

514 PERFORM ANALYSIS ON EXTRACTED EVENT RECORDS

516 CONTINUE?

FIG. 5
Extract Fields

Specify your data source, then highlight the text you would like to extract.

Specify your data source

Source type:  

Extraction Rule Preview

When you select text, we will give you a preview of the extraction rule you have created.
Or you can manually enter and/or edit an extraction rule by clicking the button below.

Create extraction rule

☐ Dim fields that are already extracted.

Filter:  

Show:  

Result type:  

FIG. 6B
Extract Fields

Specify your data source, then highlight the text you would like to extract.

Extraction Rule Preview

When you select text, we will give you a preview of the extraction rule you have created. Or you can manually enter and/or edit an extraction rule by clicking the button below.

Create extraction rule

Filter:

Show:

Result type:

Save this extraction

FIELD 1: mddby

FIELD 2: Time

FIELD 3: Time/Date

Rec: 1

Rec: 2

Rec: 3

FIELD 1: 621

FIELD 2: 622

FIELD 3: 623

Dec 12, 2012

Dec 13, 2012

Dec 14, 2012

15:1; 2.13

15:1; 2.15

15:1; 2.15

621

622

623

641

642

643

644

645

646

647

648

649

FIG. 6C
INTERFACE FOR MANAGING SPLITTABLE TIMESTAMP ACROSS EVENT RECORDS

TECHNICAL FIELD

[0001] The present invention relates generally to data selection management, and more particularly, but not exclusively, to providing a graphical user interface usable to identify splittable timestamp information across one or more locations within event records.

BACKGROUND

[0002] The rapid increase in the production and collection of machine-generated data has created large data sets that are difficult to search and/or otherwise analyze. The machine data can include sequences of records that may occur in one or more usually continuous streams. Further, machine data often represents activity made up of discrete events.

[0003] Often, search engines may receive data from various data sources, including machine data. In some cases, search engines may be configured to transform the received data in various ways prior to storing it. At least one of the transformations may include extracting field values from the received data. Sometimes the received data may be unstructured, which may make it difficult for systems to efficiently analyze the received data to determine what data may be of interest and/or how to generate a field value extraction rule. This may be especially true where the datasets are considered extremely large, such as terabytes or greater. Such large datasets may make it difficult and time consuming to analyze the data so as to be able to perform various actions on the data. For example, determining extraction rules, modification rules, or the like on such large datasets that are correct and effective may be difficult and time consuming. Improper and/or ineffective rules may result in improper values from the received data and/or omit significant values. Thus, it is with respect to these considerations and others that the present invention has been made.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Non-limiting and non-exhaustive embodiments are described with reference to the following drawings. In the drawings, like reference numerals refer to like parts throughout the various figures unless otherwise specified.

[0005] For a better understanding, reference will be made to the following Detailed Description, which is to be read in association with the accompanying drawings, wherein:

[0006] FIG. 1 illustrates a system environment in which various embodiments may be implemented;

[0007] FIG. 2A shows a rack of blade servers that may be included in various embodiments;

[0008] FIG. 2B illustrates an embodiment of a blade server that may be included in a rack of blade servers such as that shown in FIG. 2A;

[0009] FIG. 3 shows a client device that may be included in various embodiments;

[0010] FIG. 4 illustrates a network device that may be included in various embodiments;

[0011] FIG. 5 illustrates a logical flow diagram generally showing one embodiment of an overview process for identifying one or more locations within a record with splittable timestamp information usable within extraction rules; and

[0012] FIGS. 6A-C illustrate various non-limiting, non-exhaustive graphical user interfaces usable for identifying one or more locations within records with splittable timestamp information.

DETAILED DESCRIPTION

[0013] Various embodiments now will be described more fully hereinafter with reference to the accompanying drawings, which form a part hereof, and which show, by way of illustration, specific embodiments by which the invention may be practiced. The embodiments may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the embodiments to those skilled in the art. Among other things, the various embodiments may be methods, systems, media, or devices. Accordingly, the various embodiments may take the form of an entirely hardware embodiment, an entirely software embodiment, or an embodiment combining software and hardware aspects. The following detailed description is, therefore, not to be taken in a limiting sense.

[0014] Throughout the specification and claims, the following terms take the meanings explicitly associated herein, unless the context clearly dictates otherwise. The phrase “in one embodiment” as used herein does not necessarily refer to the same embodiment, though it may. Furthermore, the phrase “in another embodiment” as used herein does not necessarily refer to a different embodiment, although it may. Thus, as described below, various embodiments may be readily combined, without departing from the scope or spirit of the invention.

[0015] In addition, as used herein, the term “or” is an inclusive “or” operator, and is equivalent to the term “and/or,” unless the context clearly dictates otherwise. The term “based on” is not exclusive and allows for being based on additional factors not described, unless the context clearly dictates otherwise. In addition, throughout the specification, the meaning of “a,” “an,” and “the” include plural references. The meaning of “in” includes “in” and “on.” For example, embodiments, the following terms are also used herein according to the corresponding meaning, unless the context clearly dictates otherwise.

[0016] The term “machine data” as used herein may include data generated by machines, including, but not limited to, server logs or other types of event data, including event records. In at least one of various embodiments, machine data streams may be time stamped to create time stamped events. For example, information processing environments, such as, firewalls, routers, web servers, application servers and databases may generate streams of time series data in the form of events. In some cases, events may be generated hundreds or thousands of times per second. In some embodiments, the machine data may be unstructured data, structured data, and/or a combination thereof. Unstructured data may refer to data that does not include at least one predefined field.

[0017] The term “extraction rule” and/or “data field extraction rule” may refer to instructions that may be applied to identify and extract field values from data, such as event records. In some embodiments, extraction rule may define a field within even records from which to extract a value. In at least one of various embodiments, the extraction rules may include regular expressions. The data from which extraction
rules may be applied may include structured and/or unstructured machine data, indexed, non-indexed, event records, or other type of data.

[0018] The term "regular expression" as used herein refers to a sequence of constants and operators arranged into expressions for matching a set of strings. A regular expression is often defined as a pattern matching language which can be employed to identify character strings, for example, to select specific strings from a set of character strings. More particularly, regular expressions are often defined as a context-independent syntax that can represent a wide variety of character sets and character set orderings. In operation, regular expressions can be employed to search data based upon a predefined pattern or set of patterns. As such, this pattern matching language employs a specific syntax by which particular characters or strings are selected from a body of text. Although simple examples of regular expressions can be easily understood, oftentimes, the syntax of regular expressions is so complex that even the most experienced programmers have difficulty in understanding them. Regular expressions may be constructed using a variety of computer languages and constructs. In addition to matching, some regular expression systems offer functionality, such as, substitution, grouping, back references, or the like. Regular expressions and regular expression systems may be adapted to work with non-string data providing matching facilities for binary data.

[0019] The term "event record" may refer to computing data that is collected about an event for a computing system, including, for example, an action, characteristic, condition (or state) of the computing system. For example, such events may be about a computing system’s performance, actions taken by the computing system, or the like. Event records may be obtained from various computing log files generated by the computer’s operating system, and/or other monitoring applications. However, event records are not restricted by a file format or structure from which the event data is obtained. In various embodiments, event records may include structured and/or unstructured machine data.

[0020] The phrase "location within an event record" refers to one ore more sequential characters (e.g., a string) within the event record. The location with the event record, in some embodiments, may be delimited based on various delimiters used to separate portions of the event record. However, the location may also be delimited based on a characteristic of the data within the event record that might be used in an extraction rule; based on a starting column or position within the event record; or any of a variety of other criteria.

[0021] The following briefly describes embodiments in order to provide a basic understanding of some aspects of the invention. This brief description is not intended as an extensive overview. It is not intended to identify key or critical elements, or to delineate or otherwise narrow the scope. Its purpose is merely to present some concepts in a simplified form as a prelude to the more detailed description that is presented later.

[0022] Briefly stated, various embodiments are directed towards providing a graphical user interface usable to identify one or more locations within event records with splittable timestamp information. A display of a plurality of event records is provided to a user through a display interface device using any of a variety of formats. A splittable timestamp selector is displayed that allows the user to select one or more locations within event records as having time information that may be split across the one or more locations. For example, the user might select one location within the event records as having date information, another location as having time of day information, and yet another location as having day of the week information, or so forth. The subject innovations are not limited however to these non-limiting, non-exhaustive examples for splitting timestamp information across locations within the event records, and other arrangements and/or allocations are also allowed. Therefore, in some embodiments, the user might uniquely identify a decomposition or splitting for the timestamps. Any of a plurality of mechanisms may then be used to associate the selected locations with the split timestamp information, including, but not limited to tags, labels, or additional field header information within the event records. In other embodiments, a separate table, list, index, or the like, may be generated that associates the locations within the event records with the split timestamp information. Moreover, the graphical user interface displays such relationship, illustrating which locations within the event records are associated with which portion of the split timestamp information.

[0023] While the plurality of event records may be configured to include structured data having definable locations, such as fields, columns, or the like, based on separators, field headers, or so forth, subject innovations discussed herein are not limited to structured data event records. Selection of locations may also be performed over unstructured data event records. For example, in some embodiments, an analysis might be performed that provides extraction rules, or the like, that may identify locations within the unstructured data event records having time information. The event records may be displayed through the graphical user interface to enable the user to select locations over which to split the timestamp information.

[0024] It should be noted that while the subject innovations discussed herein disclose splitting timestamp information across locations within event records, the subject innovations are not constrained to timestamp information. Thus, in some embodiments, other splitting information might also employ similar selectors. For example, information about geographic regions might be split across various locations within event records, such as country information for one location within the event records, state or district information for another location within the event records, and city or town information for still another location within the event records. Virtually any information that can be split for use in identifying different locations within event records may be used.

Illustrative Operating Environment

[0025] FIG. 1 shows components of an environment in which various embodiments may be practiced. Not all of the components may be required to practice the various embodiments, and variations in the arrangement and type of the components may be made without departing from the spirit or scope of the various embodiments.

[0026] In at least one embodiment, cloud network 102 enables one or more network services for a user based on the operation of corresponding arrangements 104 and 106 of virtually any type of networking computing device. As shown, the networked computing devices may include extraction rule server device 112, event records server device 114, enclosure of blade servers 110, enclosure of server computers 116, super computer network device 118, and the like. Although not shown, one or more client devices may be included in
cloud network 102 in one or more arrangements to provide one or more network services to a user. Also, these arrangements of networked computing devices may or may not be mutually exclusive of each other.

[0027] In at least one of the various embodiments, extraction rule server device 112 may include module, processes, components, services, or the like, for generating extraction rules for extracting fields from event records. Further, in at least one of the various embodiments, event records server device 114 may include processes, modules, services, components, or the like, for collecting and managing data event records. In at least one of the various embodiments, event records server device 114 may employ extraction rules provided by extraction rule server 112 for managing event records, or other forms of data.

[0028] Additionally, the user may employ a plurality of virtually any type of wired or wireless networking computing devices to communicate with cloud network 102 and access at least one of the network services enabled by one or more of arrangements 104 and 106. These networking computing devices may include tablet client device 122, handheld client device 124, wearable client device 126, desktop client device 120, and the like. Although not shown, in various embodiments, the user may also employ notebook computers, server computers, microprocessor-based or programmable consumer electronics, network appliances, mobile telephones, smart telephones, pagers, radio frequency (RF) devices, infrared (IR) devices, personal Digital Assistants (PDAs), televisions, integrated devices combining at least one of the preceding devices, and the like.

[0029] One embodiment of a client device is described in more detail below in conjunction with FIG. 3. Generally, client devices may include virtually any substantially networked computing device capable of communicating over a wired, wireless, or some combination of wired and wireless network.

[0030] In various embodiments, network 102 may employ virtually any form of communication technology and topology. For example, network 102 can include local area networks Personal Area Networks (PANs), (LANs), Campus Area Networks (CANs), Metropolitan Area Networks (MANs) Wide Area Networks (WANs), direct communication connections, and the like, or any combination thereof. On an interconnected set of LANs, including those based on differing architectures and protocols, a router acts as a link between LANs, enabling messages to be sent from one to another. In addition, communication links within networks may include virtually any type of link, e.g., twisted wire pair lines, optical fibers, open air lasers or coaxial cable, plain old telephone service (POTS), wave guides, acoustic, full or fractional dedicated digital communication lines including T1, T2, T3, and T4, and/or other carrier and other wired media and wireless media. These carrier mechanisms may include E-carriers, Integrated Services Digital Networks (ISDNs), universal serial bus (USB) ports, Firewire ports, Thunderbolt ports, Digital Subscriber Lines (DSLs), wireless links including satellite links, or other communications links known to those skilled in the art. Moreover, these communication links may further employ any of a variety of digital signaling technologies, including without limit, for example, DS-0, DS-1, DS-2, DS-3, DS-4, OC-3, OC-12, OC-48, or the like. Furthermore, remotely located computing devices could be remotely connected to networks via a modem and a temporary communication link. In essence, network 102 may include virtually any communication technology by which information may travel between computing devices. Additionally, in the various embodiments, the communicated information may include virtually any kind of information including, but not limited to processor-readable instructions, data structures, program modules, applications, raw data, control data, archived data, video data, voice data, image data, text data, and the like.

[0031] Network 102 may be partially or entirely embodied by one or more wireless networks. A wireless network may include any of a variety of wireless sub-networks that may further overlay stand-alone ad-hoc networks, and the like. Such sub-networks may include mesh networks, Wireless LAN (WLAN) networks, Wireless Router (WR) mesh, cellular networks, picoc networks, PANs, Open Air Laser networks, Microwave networks, and the like. Network 102 may further include an autonomous system of intermediate network devices such as terminals, gateways, routers, switches, firewalls, load balancers, and the like, which are coupled to wired and/or wireless communication links. These autonomous devices may be operable to move freely and randomly and organize themselves arbitrarily, such that the topology of network 102 may change rapidly.

[0032] Network 102 may further employ a plurality of wired and wireless access technologies, e.g., 2nd (2G), 3rd (3G), 4th (4G), and 5th (5G) generation wireless access technologies, and the like, for mobile devices. These wired and wireless access technologies may also include Global System for Mobile communication (GSM), General Packet Radio Services (GPRS), Enhanced Data GSM Environment (EDGE), Code Division Multiple Access (CDMA), Wideband Code Division Multiple Access (WCDMA), Long Term Evolution Advanced (LTE), Universal Mobile Telecommunications System (UMTS), Orthogonal frequency-division multiplexing (OFDM), Wideband Code Division Multiple Access (W-CDMA), Code Division Multiple Access 2000 (CDMA2000), Evolution-Data Optimized (EV-DO), High Speed Downlink Packet Access (HSDPA), IEEE 802.16 Worldwide Interoperability for Microwave Access (WiMax), ultra wide band (UWB), user datagram protocol (UDP), transmission control protocol/internet protocol (TCP/IP), any portion of the Open Systems Interconnection (OSI) model protocols, Short Message Service (SMS), Multimedia Messaging Service (MMS), Web Access Protocol (WAP), Session Initiation Protocol/Real-time Transport Protocol (SIP/RTCP), or any of a variety of other wireless or wired communication protocols. In one non-limiting example, network 102 may enable a mobile device to wirelessly access a network service through a combination of several radio network access technologies such as GSM, EDGE, SMS, HSDPA, and the like.

Enclosure of Blade Servers

[0033] FIG. 2A shows one embodiment of an enclosure of blade servers 200, which are also illustrated in FIG. 1. Enclosure of blade servers 200 may include many more or fewer components than those shown in FIG. 2A. However, the components shown are sufficient to disclose an illustrative embodiment. Generally, a blade server is a stripped down server computer device with a modular design optimized to minimize the use of physical space and energy. A blade enclosure can include several blade servers and provide each with power, cooling, network interfaces, input/output interfaces, and resource management. Although not shown, an enclosure
of server computers typically includes several computers that merely require a network connection and a power cord connection to operate. Each server computer often includes redundant components for power and interfaces.

[0034] As shown in the figure, enclosure 200 contains power supply 204, and input/output interface 206, rack logic 208, several blade servers 210, 212, 214, and 216, and backplane 202. Power supply 204 provides power to each component and blade server within the enclosure. The input/output interface 206 provides internal and external communication for components and blade servers within the enclosure. Backplane 208 can enable passive and active communication of power, logic, input signals, and output signals for each blade server.

Illustrative Blade Server

[0035] FIG. 2B illustrates an illustrative embodiment of blade server 250, which may include many more or fewer components than those shown. As shown in FIG. 2A, a plurality of blade servers may be included in one enclosure that shares resources provided by the enclosure to reduce size, power, and cost.

[0036] Blade server 250 may include processor 252 which communicates with memory 256 via bus 254. Blade server 250 may also include input/output interface 290, processor-readable stationary storage device 292, and processor-readable removable storage device 294. Input/output interface 290 can enable blade server 250 to communicate with other blade servers, client devices, network devices, and the like. Interface 290 may provide wireless and/or wired communication links for blade server. Processor-readable stationary storage device 292 may include devices such as an electromagnetic storage device (hard disk), solid state hard disk (SSD), hybrid of both an SSD and a hard disk, and the like. Also, processor-readable removable storage device 294 enables processor 252 to read non-transitory storage media for storing and accessing processor-readable instructions, modules, data structures, and other forms of data. The non-transitory storage media may include flash drives, tape media, floppy media, and the like.

[0037] Memory 256 may include Random Access Memory (RAM), Read-Only Memory (ROM), hybrid of RAM and ROM, and the like. As shown, memory 256 includes operating system 258 and basic input/output system (BIOS) 260 for enabling the operation of blade server 250. In various embodiments, a general-purpose operating system may be employed such as a version of UNIX, or LINUX®, or a specialized server operating system such as Microsoft’s Windows Server® and Apple Computer’s iOSServer®.

[0038] Memory 256 may further include one or more data storage 270, which can be utilized by blade server 250 to store, among other things, applications 280 and/or other data. Data stores 270 may include program code, data, algorithms, and the like, for use by processor 252 to execute and perform actions. In one embodiment, at least some of data store 270 might also be stored on another component of blade server 250, including, but not limited to, processor-readable removable storage device 294, processor-readable stationary storage device 292, or any other processor-readable storage device (not shown). Data storage 270 may include, for example, event records 272, timestamp associations 275, and extraction rules 274. Timestamp associations 275 may include tags, labels, indices, tables, or other mechanisms usable to associate timestamp information with locations within event records.

[0039] Applications 280 may include processor executable instructions which, when executed by blade server 250, transmit, receive, and/or otherwise process messages, audio, video, and enable communication with other networked computing devices. Examples of application programs include database servers, file servers, calendars, transcoders, and so forth. Applications 280 may include, for example, extraction rule application 282, and timestamp labeler 283. In some embodiments, timestamp labeler 283 may be configured to provide a graphical user interface usable to identify locations within an event record with splittable timestamp information. Timestamp labeler 283 is illustrated as a separate application, however, it should be understood that timestamp labeler 283 may operate within another application or be called through another application. Moreover, timestamp labeler 283 may employ a process such as described below in more detail in conjunction with FIG. 5 to perform at least some of its actions. Timestamp labeler 283 may further employ graphical user interfaces, such as those discussed below in conjunction with FIGS. 6A-6C.

[0040] Human interface components (not pictured), may be remotely associated with blade server 250, which can enable remote input to and/or output from blade server 250. For example, information to a display or from a keyboard can be routed through the input/output interface 290 to appropriate peripheral human interface components that are remotely located. Examples of peripheral human interface components include, but are not limited to, an audio interface, a display, keypad, pointing device, touch interface, and the like.

Illustrative Client Device

[0041] FIG. 3 shows one embodiment of client device 300 that may include many more or less components than those shown. Client device 300 may represent, for example, at least one embodiment of client devices shown in FIG. 1.

[0042] Client device 300 may include processor 302 in communication with memory 304 via bus 328. Client device 300 may also include power supply 330, network interface 332, audio interface 350, display 350, keypad 352, illuminator 354, video interface 342, input/output interface 338, haptic interface 364, global positioning systems (GPS) receiver 358, open air gesture interface 360, temperature interface 362, camera(s) 340, projector 346, pointing device interface 366, processor-readable stationary storage device 334, and processor-readable removable storage device 336. Client device 300 may optionally communicate with a base station (not shown), or directly with another computing device. And in one embodiment, although not shown, a gyroscope may be employed within client device 300 to measuring and/or maintaining an orientation of client device 300.

[0043] Power supply 330 may provide power to client device 300. A rechargeable or non-rechargeable battery may be used to provide power. The power may also be provided by an external power source, such as an AC adapter or a powered docking cradle that supplements and/or recharges the battery.

[0044] Network interface 332 includes circuitry for coupling client device 300 to one or more networks, and is constructed for use with one or more communication protocols and technologies including, but not limited to, protocols and technologies that implement any portion of the OSI model for mobile communication (GSM), CDMA, time division mul-
multiple access (TDMA), UDP, TCP/IP, SMS, MMS, GPRS, WAP, UWB, WiMax, SIP/RTP, GPRS, EDGE, WCDMA, LTE, UMTS, OFDM, CDMA2000, EV-DO, HSDPA, or any of a variety of other wireless communication protocols. Network interface 332 is sometimes known as a transceiver, transcoding device, or network interface card (NIC).

Audio interface 356 may be arranged to produce and receive audio signals such as the sound of a human voice. For example, audio interface 356 may be coupled to a speaker and microphone (not shown) to enable telecommunication with others and/or generate an audio acknowledgement for some action. A microphone in audio interface 356 can also be used for input to or control of client device 300, e.g., using voice recognition, detecting touch based on sound, and the like.

Display 350 may be a liquid crystal display (LCD), gas plasma, electronic ink, light emitting diode (LED), Organic LED (OLED) or any other type of light reflective or light transmissive display that can be used with a computing device. Display 350 may also include a touch interface 344 arranged to receive input from an object such as a stylus or a digit from a human hand, and may use resistive, capacitive, surface acoustic wave (SAW), infrared, radar, or other technologies to sense touch and/or gestures.

Projector 346 may be a remote handheld projector or an integrated projector that is capable of projecting an image on a remote wall or any other reflective object such as a remote screen.

Video interface 342 may be arranged to capture video images, such as a still photo, a video segment, an infrared video, or the like. For example, video interface 342 may be coupled to a digital video camera, a web-camera, or the like. Video interface 342 may comprise a lens, an image sensor, and other electronics. Image sensors may include a complementary metal-oxide-semiconductor (CMOS) integrated circuit, charge-coupled device (CCD), or any other integrated circuit for sensing light.

Keypad 352 may comprise any input device arranged to receive input from a user. For example, keypad 352 may include a push button numeric dial, or a keyboard. Keypad 352 may also include command buttons that are associated with selecting and sending images.

Illuminator 354 may provide a status indication and/or provide light. Illuminator 354 may remain active for specific periods of time or in response to events. For example, when illuminator 354 is active, it may backlight the buttons on keypad 352 and stay on while the client device is powered. Also, illuminator 354 may backlight these buttons in various patterns when particular actions are performed, such as dialing another client device. Illuminator 354 may also cause light sources positioned within a transparent or translucent case of the client device to illuminate in response to actions.

Client device 300 may also comprise input/output interface 338 for communicating with external peripheral devices or other computing devices such as other client devices and network devices. The peripheral devices may include an audio headset, display screen glasses, remote speaker system, remote speaker and microphone system, and the like. Input/output interface 338 can utilize one or more technologies, such as Universal Serial Bus (USB), Infrared, WiFi, WiMax, Bluetooth™, and the like.

Haptic interface 364 may be arranged to provide tactile feedback to a user of the client device. For example, the haptic interface 364 may be employed to vibrate client device 300 in a particular way when another user of a computing device is calling. Temperature interface 362 may be used to provide a temperature measurement input and/or a temperature changing output to a user of client device 300. Open air gesture interface 360 may sense physical gestures of a user of client device 300, for example, by using single or stereo video cameras, radar, a gyroscope sensor inside a device held or worn by the user, or the like. Camera 340 may be used to track physical eye movements of a user of client device 300.

GPS transceiver 358 can determine the physical coordinates of client device 300 on the surface of the Earth, which typically outputs a location as latitude and longitude values. GPS transceiver 358 can also employ other geo-positioning mechanisms, including, but not limited to, triangulation, assisted GPS (AGPS), Enhanced Observed Time Difference (E-OTD), Cell Identifier (CI), Service Area Identifier (SAI), Enhanced Timing Advance (ETA), Base Station Sub-system (BSS), or the like, to further determine the physical location of client device 300 on the surface of the Earth. It is understood that under different conditions, GPS transceiver 358 can determine a physical location for client device 300. In at least one embodiment, however, client device 300 may, through other components, provide other information that may be employed to determine a physical location of the device, including for example, a Media Access Control (MAC) address, IP address, and the like.

Human interface components can be peripheral devices that are physically separate from client device 300, allowing for remote input and/or output to client device 300. For example, information routed as described here through human interface components such as display 350 or keyboard 352 can instead be routed through network interface 332 to appropriate human interface components located remotely. Examples of human interface peripheral components that may be remote include, but are not limited to, audio devices, pointing devices, keyboards, displays, cameras, projectors, and the like. These peripheral components may communicate over in a Pico Network such as Bluetooth™, Zigbee™ and the like. One non-limiting example of a client device with such peripheral human interface components is a wearable computing device, which might include a remote pico projector along with one or more cameras that remotely communicate with a separately located client device to sense a user’s gestures toward portions of an image projected by the pico projector onto a reflected surface such as a wall or the user’s hand.

A client device may include a browser application that is configured to receive and to send web pages, web-based messages, graphics, text, multimedia, and the like. The client device's browser application may employ virtually any programming language, including a wireless application protocol messages (WAP), and the like. In at least one embodiment, the browser application is enabled to employ Handheld Device Markup Language (HDML), Wireless Markup Language (WML), WMLScript, JavaScript, Standard Generalized Markup Language (SGML), HyperText Markup Language (HTML), eXtensible Markup Language (XML), HTML5, and the like.

Memory 304 may include RAM, ROM, and/or other types of memory. Memory 304 illustrates an example of computer-readable storage media (devices) for storage of information such as computer-readable instructions, data structures, program modules or other data. Memory 304 may store BIOS 308 for controlling low-level operation of client device 300. The memory may also store operating system 306.
for controlling the operation of client device 300. It will be appreciated that this component may include a general-purpose operating system such as a version of UNIX, or LINUX™, or a specialized mobile computer communication operating system such as Windows Phone™, or the Symbian® operating system. The operating system may include, or interface with a Java virtual machine module that enables control of hardware components and/or operating system operations via Java application programs.

[0057] Memory 304 may further include one or more data storage 310, which can be utilized by client device 300 to store, among other things, applications 320 and/or other data. For example, data storage 310 may also be employed to store information that describes various capabilities of client device 300. The information may then be provided to another device based on any of a variety of events, including being sent as part of a header during a communication, sent upon request, or the like. Data storage 310 may also be employed to store social networking information including address books, buddy lists, aliases, user profile information, or the like. Data storage 310 may further include program code, data, algorithms, and the like, for use by a processor, such as processor 302 to execute and perform actions. In one embodiment, at least some of data storage 310 may also be stored on another component of client device 300, including, but not limited to, non-transitory processor-readable removable storage device 336, processor-readable stationary storage device 334, or even external to the client device.

[0058] Applications 320 may include computer executable instructions which, when executed by client device 300, transmit, receive, and/or otherwise process instructions and data. Applications 320 may include, for example, extraction rule application 322. Other examples of application programs include calendars, search programs, email client applications, IM applications, SMS applications, Voice Over Internet Protocol (VOIP) applications, contact managers, task managers, transcoders, database programs, word processing programs, security applications, spreadsheet programs, games, search programs, and so forth.

[0059] Extraction rule application 322 may be configured to enable creation of extraction rules and to display results of the extraction rules to a user. In at least one embodiment, extraction rule application 322 may interact with and/or be employed through a web browser. In some embodiments, embodiments, extraction rule application 322 may enable a user to input and/or edit one or more extraction rules. In other embodiments, extraction rule application 322 may display a plurality of event records to a user, values extracted from the event records using the extraction rule, statistics about the extracted values, or the like.

[0060] Also shown is timestamp labeler 323, which is configured to enable client device 300 to display and use a graphical user interface to identify one or more locations within an event record that may have time information, and to further allow the locations to be associated with splittable timestamp information. Such splittable timestamp information may then be usable to perform any of a variety of related actions upon the event records, including, but not limited to performing sorts on the event records, or locations within the event records; performing extractions of information within the event records or locations within the event records; or performing any of a variety of analysis on the event records.

[0061] While timestamp labeler 323 is illustrated as within extraction rule application 322, this need not be the case in other embodiments, and thus should not be construed as limiting the subject innovations. For example, timestamp labeler 323 may operate as a separate application, called from another application, or even operate on another network device over a network. In some embodiments timestamp labeler 323 is configured to provide graphical user interfaces such as those discussed in more detail below in conjunction with FIGS. 6A-6C, and further employ a process such as discussed below in conjunction with FIG. 5.

Illustrative Network Device

[0062] FIG. 4 shows one embodiment of network device 400 that may be included in a system implementing the invention. Network device 400 may include many more or less components than those shown in FIG. 4. However, the components shown are sufficient to disclose an illustrative embodiment for practicing the present invention. Network device 400 may represent, for example, one embodiment of at least one of network device 112, 114, or 120 of FIG. 1.

[0063] As shown in the figure, network device 400 may include a processor 402 in communication with a memory 404 via a bus 428. Network device 400 may also include a power supply 430, network interface 432, audio interface 456, display 450, keyboard 452, input/output interface 438, processor-readable stationary storage device 434, processor-readable removable storage device 436, and pointing device interface 458. Power supply 430 provides power to network device 400.

[0064] Network interface 432 may include circuitry for coupling network device 400 to one or more networks, and is constructed for use with one or more communication protocols and technologies including, but not limited to, protocols and technologies that implement any portion of the Open Systems Interconnection model (OSI model), GSM, CDMA, time division multiple access (TDMA), UDP, TCP/IP, SMS, MMS, GPRS, WAP, UWB, WiMax, SIP/RT, or any of a variety of other wired and wireless communication protocols. Network interface 432 is sometimes known as a transceiver, transceiving device, or network interface card (NIC). Network device 400 may optionally communicate with a base station (not shown), or directly with another computing device.

[0065] Audio interface 456 is arranged to produce and receive audio signals such as the sound of a human voice. For example, audio interface 456 may be coupled to a speaker and microphone (not shown) to enable telecommunication with others and/or generate an audio acknowledgement for some action. A microphone in audio interface 456 can also be used for input to or control of network device 400, for example, using voice recognition.

[0066] Display 450 may be a liquid crystal display (LCD), gas plasma, electronic ink, light emitting diode (LED), Organic LED (OLED) or any other type of light reflective or light transmissive display that can be used with a computing device. Display 450 may be a handheld projector or pico projector capable of projecting an image on a wall or other object.

[0067] Network device 400 also may also comprise input/output interface 438 for communicating with external devices not shown in FIG. 4. Input/output interface 438 can utilize one or more wired or wireless communication technologies, such as USB™, Firewire™, WiFi, WiMax, Thunderbolt™, Infrared, Bluetooth™, Zigbee™, serial port, parallel port, and the like.
Human interface components can be physically separate from network device 400, allowing for remote input and/or output to network device 400. For example, information routed as described here through human interface components such as display 450 or keyboard 452 can instead be routed through the network interface 432 to appropriate human interface components located elsewhere on the network. Human interface components can include any component that allows the computer to take input from, or send output to, a human user of a computer.

Memory 404 may include RAM, ROM, and/or other types of memory. Memory 404 illustrates an example of computer-readable storage media (devices) for storage of information such as computer-readable instructions, data structures, program modules or other data. Memory 404 may store BIOS 408 for controlling low-level operation of network device 400. The memory may also store operating system 406 for controlling the operation of network device 400. It will be appreciated that this component may include a general-purpose operating system such as a version of UNIX, or LINUX™, or a specialized operating system such as Microsoft Corporation’s Windows® operating system, or the Apple Corporation’s iOS® operating system. The operating system may include, or interface with a Java virtual machine module that enables control of hardware components and/or operating systems operations via Java application programs.

Memory 404 may further include one or more data storage 410, which can be utilized by network device 400 to store, among other things, applications 420 and/or other data. For example, data storage 410 may also be employed to store information that describes various capabilities of network device 400. The information may then be provided to another device based on any of a variety of events, including being sent as part of a header during a communication, sent upon request, or the like. Data storage 410 may also be employed to store social networking information including address books, buddy lists, aliases, user profile information, or the like. Data stores 410 may further include program code, data, algorithms, and the like, for use by a processor, such as processor 402 to execute and perform actions. In one embodiment, at least some of data store 410 might also be stored on another component of network device 400, including, but not limited to, non-transitory media inside processor-readable removable storage device 436, processor-readable stationary storage device 434, or any other computer-readable storage device within network device 400, or even external to network device 400.

Data storage 410 may include, for example, event records 412 and extraction rules 416. In some embodiments, event records 412 may store data, including a plurality of event records. In at least one of various embodiments, event records 412 may be stored by event records server device 114 of FIG. 1. Extraction rules 416 may include one or more extensions rules. These extraction rules may be automatically created based on a user selection of text, input by a user, and/or otherwise provided to the system. In at least one embodiment, extraction rules 416 may be stored and/or otherwise processed by extraction rule server device 112 of FIG. 1. Further, data storage 410 may also include timestamp associations 413, where such associations might include tags, labels, indices, tables, lists, or the like. However, in other embodiments, modifications might be made to event records stored within event records 412 to indicate timestamp associations, including, modifying event records to include tags, labels, headers, additional fields, field information, or the like.

Applications 420 may include computer executable instructions which, when executed by network device 400, transmit, receive, and/or otherwise process messages (e.g., SMS, MMS, Instant Message (IM), email, and/or other messages), audio, video, and enable telecommunication with another user of another client device. Other examples of application programs include calendars, search programs, email client applications, IM applications, SMS applications, Voice Over Internet Protocol (VOIP) applications, contact managers, task managers, transcoders, database programs, word processing programs, security applications, spreadsheet programs, games, search programs, and so forth. Applications 420 may include, for example, extraction rule application 422 and timestamp label 423.

Extraction rule application 422 may be configured to enable creation of extraction rules and to display results of the extraction rules to a user. In at least one embodiment, extraction rule application 422 may interact with a client device for enabling a user to input and/or edit one or more extraction rules. In other embodiments, extraction rule application 422 may enable a client device to display a plurality of event records to a user, values extracted from the event records using the extraction rule, statistics about the extracted values, or the like. In at least one embodiment, extraction rule application 422 may interact with event records 412 and/or extraction rules 416 to access and/or store event records and/or extraction rules, respectively. In some embodiments, extraction rule application 422 may be employed by extraction rule server device 112 of FIG. 1.

Timestamp labeler 423 is configured to provide a graphical user interface usable to identify one or more locations within event records with splittable timestamp information. A display of a plurality of event records is provided to a user through the graphical user interface using any of a variety of formats, including those described below in conjunction with FIGS. 6-8. A splittable timestamp selector is displayed within the graphical user interface that allows the user to select one or more locations within event records as having time related information that may be split across the one or more locations. The splittable timestamp information may then be associated with respective locations within the event records using any of a variety of mechanisms. The associations may be stored such that it may later be used by extraction rules, sort applications, and/or any of a variety of applications in which time information may be used. For example, timestamp labeler 422 might store the associations in event records 412, and/or in timestamp associations 413. Timestamp labeler 424 may employ a process such as described below in conjunction with FIG. 5.

General Operation

The operation of certain aspects of the invention will now be described with respect to FIG. 5. FIG. 5 illustrates a logical flow diagram generally showing one embodiment of an overview process for identifying one or more locations within an event record with splittable timestamp information. Process 500 of FIG. 5 may be implemented within one or more client devices of FIG. 1, blade server 250 of FIG. 20, and/or network device 400 of FIG. 1.

Process 500 begins, after a start block, at block 502, where a plurality of event records are received, and one or
more of the event records are displayed using a graphical user interface (GUI). The GUI may be implemented using any of a variety of mechanisms, and is not constrained to any particular mechanism for displaying the one or more event records. In some embodiments, the GUI may be displayed to a user of a client device, such as described above in conjunction with FIGS. 1 and 3. However, the GUI may also be configured to be displayed using any of a variety of other devices as well. Moreover, the display of the one or more event records may use any of a variety of formats and/or arrangements. For example, event records may be displayed in a table format having rows and columns. In such a display, each event record displayed might be a displayed row, while fields or locations within the event record are columns. In other embodiments, each event record displayed might be a column, while fields or locations within the event records are rows. As discussed further below, other arrangements may also be used.

[0077] Process 500 then flows to block 504, where the GUI also displays a splittable timestamp selector. The splittable timestamp selector might be represented as a pull down menu structure, a push button, a drag/drop selector, or any of a variety of other selector mechanisms, including a combination of one or more selector mechanisms. The splittable timestamp selector is configured to allow the user to identify locations within a displayed event record having portions of time information for which the user may select. For example, one location of the event record might include month/day/year information, while another location within the event record might include day of the week information, time of day information, or so forth. Clearly, an event record might include locations that include combinations of such time information, and/or other types of time information. Therefore, subject innovations are not limited to a particular structure, type, or combination of time information. Virtually any time information may be included for which a user might select.

[0078] In one non-limiting example, a user might identify locations within an event record having time information that is distributed across different fields or locations within an event record. For example, one field or location within an event record might include time of day information in the form of time that is local to a source of the event record, and another location that includes universal time of day information. Another location of the event record might include, however, month/day/year information. Thus, time information might be distributed across different locations within an event record. Some of these locations within the event record however might not include a label, tag, header, or other type of indication that the content includes time information. The user might therefore wish to identify such locations as having a particular type of time information. Using the splittable timestamp selector within the GUI, the user may drag, slide, or otherwise identify and select locations within the event record as having time information, and what type of time information. The splittable timestamp selector allows the user to split timestamp information across different locations within the event record. The GUIs discussed below in conjunction with FIGS. 6A-C illustrate non-limiting examples of performing such selections.

[0079] Process 500 then moves to block 506 where as the user selects locations with splittable timestamp information, the splittable timestamp information is associated with the selected locations. This association may be accomplished using a variety of mechanisms. For example, a new field, header, tag, label, or the like might be automatically inserted in the event records, event record headers, or the like, that include the splittable timestamp information. However, in other embodiments, information about the selected locations might be inserted into a table, list, index structure, or the like, along with the associated splittable timestamp information. For example, the location within the event records might be identified as characters 26-31 and as having time information to be associated with the splittable timestamp of Month (2 characters), Day (2 characters), and Year (2 characters). Such information may also be included in a table, list, index structure, or the like, that might be maintained separately, within another event record, or using any of a variety of other mechanisms.

[0080] Process 500 flows next to decision block 508 where a determination is made whether more splittable timestamp information is to be selected and associated with locations within the event records. If so, processing flows back to block 504 to continue until no more selections are performed. Processing then continues to optional block 510.

[0081] At block 510, a user may create an extraction rule that includes splittable timestamps within the rule. For example, the user might select event records where the MM/DD/YY time information identified using the splittable timestamp, is greater than some value. As noted, any of a variety of other extraction criteria may be employed. As such, the subject innovations are not limited by this example. Proceeding to block 512, the extraction rule having splittable timestamp information is then used to extract event records that satisfy the extraction rule. Continuing to block 514, any of a variety of analyses might be then performed on the extracted event records.

[0082] Process 500 then flows to decision block 516, where a determination is made whether to continue identifying and selecting locations within event records with splittable timestamp information. If so, processing branches back to block 504; otherwise, processing may return to a calling process.

[0083] It will be understood that each block of the flowchart illustration, and combinations of blocks in the flowchart illustration, can be implemented by computer program instructions. These program instructions may be provided to a processor to produce a machine, such that the instructions, which execute on the processor, create means for implementing the actions specified in the flowchart block or blocks. The computer program instructions may be executed by a processor to cause a series of operational steps to be performed by the processor to produce a computer-implemented process such that the instructions, which execute on the processor to provide steps for implementing the actions specified in the flowchart block or blocks. The computer program instructions may also cause at least some of the operational steps shown in the blocks of the flowchart to be performed in parallel. Moreover, some of the steps may also be performed across more than one processor, such as might arise in a multi-processor computer system. In addition, one or more blocks or combinations of blocks in the flowchart illustration may also be performed concurrently with other blocks or combinations of blocks, or even in a different sequence than illustrated.

[0084] Accordingly, blocks of the flowchart illustration support combinations of means for performing the specified actions, combinations of steps for performing the specified actions and program instruction means for performing the specified actions. It will also be understood that each block of the flowchart illustration, and combinations of blocks in the
flowchart illustration, can be implemented by special purpose hardware-based systems, which perform the specified actions or steps, or combinations of special purpose hardware and computer instructions.

NON-LIMITING, NON-EXHAUSTIVE EXAMPLES OF GRAPHICAL USER INTERFACES

[0085] FIGS. 6A-C illustrate various non-limiting, non-exhaustive graphical user interfaces usable for identifying/selecting one or more locations within event records with splittable timestamp information.

[0086] GUIs 600A-C of FIGS. 6A-C are directed towards providing examples of GUIs that may be used to display one or more event records and to select locations within the event records as having time information. The GUIs further display a splittable timestamp selector that may be used to select locations within the event records as having time information. The splittable timestamp selector may be used to identify the type of time information within the selected location. This splittable timestamp information may then be associated with the selected locations as discussed above.

[0087] GUI 600A of FIG. 6A illustrates event records 612-614, within section 608A. Other sections within GUI 600A may also be displayed, including data source 602, which indicates a source of the event records; extraction rule preview 604, which may be used to create an extraction rule, and input 606 usable to enable the user to define a specific filter to apply to the event records (e.g., the user may filter the event records to display those event records that were recorded on a particular day). In other embodiments, input 606 may also enable a user to select how the event records are displayed.

[0088] As is further shown in FIG. 6A, event records 612-614 are displayed in a "by row" format, where each row represents one event record. Also, shown as columns are locations 630-637 for each of event records 612-614. Where tags, labels, or field headers are available, they are further illustrated in row 610.

[0089] Splittable timestamp selector 620 is shown in FIG. 6A, having selection arrows that may be employed to select split time information. Splittable timestamp selector 620 may be clicked on, dragged, or otherwise moved, relocated over one or more columns/locations of the displayed event records 612-614 to select a location having time information. The selection arrows may be used to select a split time for the selected location. In one non-limiting, non-exhaustive example, a user might drag splittable timestamp selector 620 over location 631 and employ the selection arrows to identify that location 631 has month/day/year (MM/DD/YY) time information. A result of such actions is shown as splittable timestamp selection 621. Similar actions may be repeated, resulting in splittable timestamp selection 622 showing location 633 having time of day, in Zulu time, and splittable timestamp selection 623 showing location 636 having weekday time information. Thus, using GUI 600A, the user may employ splittable timestamp selector 620 multiple times, to select multiple locations within the displayed event records as having split time information. However, in other embodiments, splittable timestamp selection 621 might be dragged to another location to enable splitting of, for example, the MM/DD/YY time information. Thus, in some embodiments, a user might split the MM/DD/YY time information across two or more locations, such as MM for one location, DD for another location, and YY for still another location. Similarly, splittable timestamp selection 622 might also be further split. Thus, in some embodiments, the splittable timestamp selection 622 might be dragged over multiple locations, with selections made using splittable timestamp selection 622 as sort of an extension of splittable timestamp selector 620. Thus, in this manner, designating splits of time across locations within event records may be performed in a variety of ways.

[0090] It should be clear that any of a variety of other locations, and/or split time information may be selected. For example, in one embodiment, splittable timestamp selector 620 might allow a user to select to enter a definition of split time for locations. That is, in some embodiments, the user might define a unique splitting of time, or even a previously undefined timestamp designation. Moreover, in some embodiments, when a location within the displayed event records is selected, an association is made between the split time information and the selected location to indicate that the selected location has time information as indicated by the selected identifier (e.g., MM/DD/YY, time of day: Zulu, or weekday). Moreover, it should be understood that such association between the split time information and the location might be applied over a plurality of event records, including those event records that are displayed, or alternatively, over a subset of event records, such as event records extracted from the plurality of event records based on an extraction rule, or the like. In any event, the splittable timestamp/location associations may then be used to perform any of a variety of operations upon the event records.

[0091] As noted above, subject innovations are not limited by how an event record, event record locations, and splittable timestamp information is displayed. Thus, while FIG. 6A illustrates event records 612-614 in rows, and columns as locations/fields within the event records, other arrangements may be used. For example, in some embodiments, event records might be displayed in columns, while locations/fields with the event records might be displayed in rows. Splittable timestamp information may then be displayed in a column, and aligned with respectively selected locations/rows within the event records.

[0092] For example, some data might have event records with too many extracted fields to readily display as columns. Therefore, in some embodiments, the fields of each event record might be displayed with one field per row for each event record, and then displaying event records one under another. A similar concept might include moving the splittable timestamp information between fields to indicate the one from which a timestamp might be extracted, or otherwise selected; however, in this instance the timestamp (or portions thereof) might move up or down between the fields rather than across columns.

[0093] FIG. 6B shows another non-limiting, non-exhaustive arrangement of event records, locations/fields within event records, and how splittable timestamp information might be displayed. In this example, GUI 600B shows portions of event records 612-613. The event records are shown in a single column, one event record below another event record. Shown for event record 612 are locations 631A and 633A, while at least location 631B of event record 613 is displayed. A scrolling tool is shown next to each event record, allowing scrolling within each event record, to display respective locations/fields within an event record. Moreover a global scrolling tool is shown that allows for scrolling over the event records. Splittable timestamp selector 620 may again be used to select locations within the displayed event.
records as having time information, as discussed above. Thus, as shown, FIG. 6B shows results of a selection of field/location 631A as having split time information of MMDDYY, as shown by splittable timestamp selection 621A. In some embodiments, such selection in one event record may be automatically reflected within other event records. Thus, in some embodiments, splittable timestamp selection 621B might automatically be displayed to reflect selections of a similar field/location within another event record based on one selection. Also shown is splittable timestamp selection 622A for location 633A of event record 612. While not displayed, a similar automatic selection might occur for event record 613, and/or other event records.

[0094] FIG. 6C illustrates still another non-limiting, non-exhaustive arrangement of event records, locations/fields within event records, and how splittable timestamp information might be displayed. In this example, GUI 600C, event records are again displayed in row format, as in 612A, 613A, and so forth. However, a separate row is also shown for fields/locations selected as having time information. Thus, as shown row 641 illustrates that field 1 (location 631) of the event records 612-613 (as displayed by event records 612A and 613A) has time information as shown by splittable timestamp selection 621. Similarly, row 641 also shows that field 3 (location 633) of the event records 612-613 (and displayed as event records 612B and 613B) has time information as shown by splittable timestamp selection 622. In this example, then, GUI 600C might display multiple instances of an event record, as rows, with other rows indicating which field/location within the event records are selected using the splittable timestamp selector 620.

[0095] Other arrangements or structures, formats, or the like, may be used to display within a GUI event records and locations within the event records such that a user might select locations having time information using a splittable timestamp selector. Thus, embodiments should not be construed as being limited by any particular arrangement of event records, type of splittable timestamp selectors, or mechanisms used to select locations within event records.

[0096] The above specification, examples, and data provide a complete description of the composition, manufacture, and use of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

1-30. (canceled)
31. A method, comprising:
   receiving raw data;
   generating one or more events for a computing system, wherein each event includes a portion of the raw data;
   causing generation of a graphical interface on a computing device, wherein the graphical interface displays at least one of the events and a timestamp selection tool, and wherein a timestamp selection tool is a graphical interface tool that enables a user to graphically designate one or more sub-portions of raw data within an event to be extracted and used to generate a timestamp for the event;
   receiving input corresponding to a designation of the one or more sub-portions of raw data within the event, wherein the designation is made using the timestamp selection tool;
   dynamically generating and storing an extraction rule for determining a timestamp for the event from the designated one or more sub-portions of raw data in the event;
   for each of the one or more events, applying the extraction rule to the portion of raw data in the event to generate a timestamp for the event;
   storing each of the one or more events using the extracted timestamp for that event;
   wherein the method is performed by one or more computing devices.
32-39. (canceled)
40. A system for managing resources, comprising:
   at least one network device, comprising:
   a processor; and
   a non-transitory computer-readable storage medium containing instructions configured to cause the processor to perform operations including:
   generating one or more events for a computing system, wherein each event includes a portion of the raw data;
   causing generation of a graphical interface on a computing device, wherein the graphical interface displays at least one of the events and a timestamp selection tool, and wherein a timestamp selection tool is a graphical interface tool that enables a user to graphically designate one or more sub-portions of raw data within an event to be extracted and used to generate a timestamp for the event;
   receiving input corresponding to a designation of the one or more sub-portions of raw data within the event, wherein the designation is made using the timestamp selection tool;
   dynamically generating and storing an extraction rule for determining a timestamp for the event from the designated one or more sub-portions of raw data in the event;
   for each of the one or more events, applying the extraction rule to the portion of raw data in the event to generate a timestamp for the event;
store each of the one or more events using the extracted
timestamp for that event.
60. (canceled)
61. The method of claim 31, wherein receiving input cor-
responding to the designation of the one or more sub-portions of
raw data comprises receiving input corresponding to the
designation of at least two portions of raw data using the
timestamp selection tool.
62. The method of claim 31, wherein receiving input cor-
responding to the designation of the one or more sub-portions of raw data comprises receiving input corresponding to the
designation of two portions of raw data using the timestamp
selection tool, wherein the timestamp selection tool is split
into two graphical user interface elements to designate the
two portions of raw data.
63. The method of claim 31, wherein the event for which the
timestamp selection tool is used to designate one or more sub-portions of raw data includes time information that is not
extracted to use for generating the timestamp for that event.
64. The method of claim 31, wherein the raw data includes
unstructured data.
65. The method of claim 31, wherein the raw data includes
machine data.
66. The method of claim 31, further comprising using one of
a tag, a label, or a header to create an association between the
timestamp and the one or more sub-portions of raw data within the event.
67. The method of claim 31, further comprising using one of
a table, a list, or an index to create an association between the
timestamp and the one or more sub-portions of raw data within the event.
68. The method of claim 31, wherein each of the one or more sub-portions of raw data designated in the event by the
timestamp selection tool includes one or more of a year, a
month, a day, and a time of day.
69. The method of claim 31, wherein at least one of the one or more sub-portions of raw data corresponds to a field that
defines a location across multiple events for a category of time
information.
70. The system of claim 40, wherein receiving input cor-
responding to the designation of the one or more sub-portions of raw data comprises receiving input corresponding to the
designation of at least two portions of raw data using the
timestamp selection tool.
71. The system of claim 40, wherein receiving input cor-
responding to the designation of the one or more sub-portions of raw data comprises receiving input corresponding to the
designation of two portions of raw data using the timestamp
selection tool, wherein the timestamp selection tool is split
into two graphical user interface elements to designate the
two portions of raw data.
72. The system of claim 40, wherein the event for which the
timestamp selection tool is used to designate one or more sub-portions of raw data includes time information that is not
extracted to use for generating the timestamp for that event.
73. The system of claim 40, wherein the raw data includes
unstructured data.
74. The system of claim 40, wherein the raw data includes
machine data.
75. The system of claim 40, wherein the operations further
comprise using one of a tag, a label, or a header to create an association between the timestamp and the one or more sub-portions of raw data within the event.
76. The system of claim 40, wherein the operations further
comprise using one of a table, a list, or an index to create an association between the timestamp and the one or more sub-portions of raw data within the event.
77. The system of claim 40, wherein each of the one or more sub-portions of raw data designated in the event by the
timestamp selection tool includes one or more of a year, a
month, a day, and a time of day.
78. The system of claim 40, wherein at least one of the one or more sub-portions of raw data corresponds to a field that
defines a location across multiple events for a category of time
information.
79. The computer-program product of claim 49, wherein the
instructions is configured to further cause the data pro-
cessing apparatus to receive input corresponding to the design-
ation of at least two portions of raw data using the time-
s tamp selection tool.
80. The computer-program product of claim 49, wherein the
instructions is configured to further cause the data pro-
cessing apparatus to receive input corresponding to the design-
ation of two portions of raw data using the timestamp
selection tool, wherein the timestamp selection tool is split
into two graphical user interface elements to designate the
two portions of raw data.
81. The computer-program product of claim 49, wherein the
event for which the timestamp selection tool is used to
designate one or more sub-portions of raw data includes time
information that is not extracted to use for generating the
timestamp for that event.
82. The computer-program product of claim 49, wherein the
raw data includes unstructured data.
83. The computer-program product of claim 49, wherein the
raw data includes machine data.
84. The computer-program product of claim 49, wherein the
instructions is configured to further cause the data pro-
cessing apparatus to use one of a tag, a label, or a header
to create an association between the timestamp and the one or more sub-portions of raw data within the event.
85. The computer-program product of claim 49, wherein the
instructions is configured to further cause the data pro-
cessing apparatus to use one of a table, a list, or an index
to create an association between the timestamp and the one or
more sub-portions of raw data within the event.
86. The computer-program product of claim 49, wherein each of the one or more sub-portions of raw data designated in the event by the timestamp selection tool includes one or more of a year, a month, a day, and a time of day.
87. The computer-program product of claim 49, wherein at
least one of the one or more sub-portions of raw data corre-
sponds to a field that defines a location across multiple events for a category of time information.

* * * * *