(19) CONFEDERAZIONE SVIZZERA
ISTITUTO FEDERALE DELLA PROPRIETÀ INTELLETTUALE

(11) CH 718 167 B1

(51) Int. Cl.: G06F 21/56 (2013.01)

Brevetto d'invenzione rilasciato per la Svizzera ed il Liechtenstein
Trattato sui brevetti, del 22 dicembre 1978, fra la Svizzera ed il Liechtenstein

(12) FASCICOLO DEL BREVETTO

(21) Numero della domanda: 070470/2021

(22) Data di deposito: 29.10.2021

(43) Domanda pubblicata: 30.06.2022

(30) Priorità: 23.12.2020 US 63/130,065
09.08.2021 US 17/396,905

(24) Brevetto rilasciato: 14.03.2025

(45) Fascicolo del brevetto pubblicato: 14.03.2025

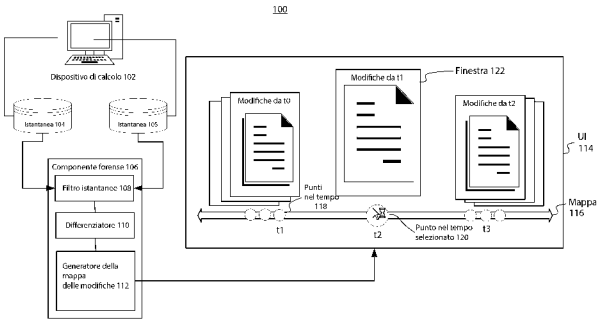
(73) Titolare/Titolari:
Acronis International GmbH, Rheinweg 9
8200 Schaffhausen (CH)

(72) Inventore/Inventori:
Serguei Beloussov, 8200 Schaffhausen (CH)
Stanislav Protasov, 8200 Schaffhausen (CH)
Candid Wüest, 8200 Schaffhausen (CH)
Nikolay Grebennikov, 8200 Schaffhausen (CH)

(74) Mandatario:
Stefano Sinigaglia c/o M. Zardi & Co. SA, Via Pioda 6
6900 Lugano (CH)

(54) Metodo per il riferimento incrociato di instantanee forensi nel tempo per l'analisi delle cause alla radice

(57) L'invenzione concerne un metodo per il riferimento incrociato di istantanee (104, 105) forensi nel tempo. Il metodo comprende la ricezione di una prima istantanea di un dispositivo di calcolo nel primo tempo e di una seconda istantanea nel secondo tempo e l'applicazione di un filtro predefinito (108) alla prima istantanea e alla seconda istantanea, il quale filtro predefinito include un elenco di file che devono essere estratti da ogni istantanea. Il metodo comprende, successivamente all'applicazione del filtro predefinito (108), l'identificazione di differenze nell'elenco dei file estratti dalla prima istantanea e dalla seconda istantanea. Il metodo comprende la creazione di una mappa (116) delle modifiche per il dispositivo di calcolo che comprenda le differenze nell'elenco dei file per un periodo di tempo, il quale periodo di tempo includa il primo tempo e il secondo tempo e l'emissione della mappa delle modifiche in un'interfaccia utente.



Descrizione

RIFERIMENTO INCROCIATO A DOMANDE CORRELATE

[0001] La presente domanda di brevetto rivendica il vantaggio della domanda di brevetto non provvisoria statunitense n. 17/396,905, depositata il 9 agosto 2021, che rivendica a sua volta il vantaggio della domanda di brevetto provvisoria statunitense n. 63/130,065, depositata il 23 dicembre 2020, entrambe accluse a titolo di riferimento.

CAMPO DELLA TECNOLOGIA

[0002] La presente divulgazione si riferisce al campo della sicurezza dei dati e, più nello specifico, a un metodo per il riferimento incrociato di istantanee forensi nel tempo.

ANTEFATTO

[0003] Dato che oggi si fa sempre più affidamento sull'informatica digitale, è aumentato parallelamente il numero di crimini informatici quali hackeraggio, sottrazione di dati e attacchi malware. Di conseguenza, è divenuto necessario salvare ulteriori informazioni riguardo ai dati presenti in un sistema, creando copie di backup che possano essere utilizzate per condurre indagini riguardo a tali crimini informatici. I tecnici forensi possono utilizzare tali informazioni supplementari per determinare l'origine di un attacco e rilevare tracce ed elementi residui dell'attacco su un sistema.

[0004] Le indagini forensi, tuttavia, non hanno in genere accesso al contenuto di file e di memorie risalenti a punti nel tempo antecedenti il momento in cui si è verificato il crimine informatico. Ciò limita l'efficienza dell'analisi poiché non è possibile visualizzare la cronologia della configurazione del sistema, esclusioni nel software anti-virus, errori di impostazione da parte del tecnico ecc. Inoltre, le soluzioni SIEM (security information and event management) e EDR (endpoint detection and response) possono solo fornire indicazioni e registrazioni di alto livello di quanto è accaduto, ma non il contenuto di file fondamentali come i file di configurazione. Senza contare che l'utilizzo di tradizionali punti di ripristino di backup per ripristinare e confrontare file è un processo che richiede molto tempo e una notevole quantità di spazio su disco.

[0005] Sussiste pertanto la necessità di offrire agli investigatori informazioni essenziali associate a un crimine informatico in modo efficiente.

COMPENDIO

[0006] Un metodo per il riferimento incrociato di istantanee forensi nel tempo secondo la presente invenzione è rivendicato nella rivendicazione 1. Forme di realizzazione preferite del metodo secondo la presente invenzione sono date nelle rivendicazioni da 2 a 7.

[0007] Per ovviare a queste lacune, alcuni esempi della divulgazione descrivono il metodo per il riferimento incrociato di istantanee forensi nel tempo. In un esempio, il metodo può comprendere la ricezione di una prima istantanea di un dispositivo di calcolo in un primo tempo e di una seconda istantanea del dispositivo di calcolo in un secondo tempo. Il metodo può comprendere l'applicazione di un filtro predefinito alla prima istantanea e alla seconda istantanea, il quale filtro predefinito includa un elenco di file che devono essere estratti da ogni istantanea. Il metodo può comprendere, successivamente all'applicazione del filtro predefinito, l'identificazione di differenze nell'elenco dei file estratti dalla prima istantanea e dalla seconda istantanea. Il metodo può comprendere la creazione di una mappa delle modifiche per il dispositivo di calcolo che comprenda le differenze nell'elenco dei file per un periodo di tempo, il quale periodo di tempo includa il primo tempo e il secondo tempo e l'emissione di una mappa delle modifiche in un'interfaccia utente.

[0008] In alcuni esempi, il metodo può comprendere la ricezione di una terza istantanea del dispositivo di calcolo in un terzo tempo, l'applicazione del filtro predefinito alla terza istantanea, l'identificazione di differenze nell'elenco dei file estratti dalla seconda istantanea e dalla terza istantanea e la modifica della mappa delle modifiche per il dispositivo di calcolo per includere inoltre differenze nell'elenco dei file nel terzo tempo, il quale periodo di tempo comprenda anche il terzo tempo.

[0009] In alcuni esempi, le differenze nell'elenco dei file nel terzo tempo sono in relazione al secondo tempo.

[0010] In alcuni esempi, le differenze nell'elenco dei file nel terzo tempo sono in relazione al primo tempo.

[0011] In alcuni esempi, la mappa delle modifiche viene emessa visivamente in un'interfaccia utente sotto forma di una sequenza temporale con una pluralità di punti nel tempo selezionabili, ciascuno dei quali rappresenta un'istantanea del dispositivo di calcolo. Il metodo può comprendere la ricezione di una selezione di un punto nel tempo e la generazione di una finestra con rispettive differenze tra un'istantanea filtrata, associata al punto nel tempo e una precedente istantanea filtrata.

[0012] In alcuni esempi, il punto nel tempo selezionato è il secondo tempo associato alla seconda istantanea e la finestra presenta le differenze nell'elenco dei file estratti dalla prima istantanea e dalla seconda istantanea.

[0013] In alcuni esempi, la finestra è interattiva e presenta un'analisi di approfondimento (drill-down) per ogni file nelle rispettive differenze.

[0014] In alcuni esempi, il metodo può comprendere l'emissione della mappa delle modifiche nell'interfaccia utente in risposta al rilevamento di un errore nel dispositivo di calcolo.

[0015] In alcuni esempi, l'emissione della mappa delle modifiche comprende inoltre la trasmissione di un avviso a un organo di indagine forense, il quale avviso comprende l'accesso alla mappa delle modifiche.

[0016] In alcuni esempi, la mappa delle modifiche indica le modifiche apportate dall'utente e le modifiche apportate da un soggetto non autorizzato, e il metodo può comprendere il filtraggio della mappa delle modifiche in modo da non mostrare le modifiche apportate dall'utente.

[0017] In alcuni esempi, il filtraggio della mappa delle modifiche per non mostrare le modifiche apportate dall'utente comprende la classificazione di ogni variazione nella mappa delle modifiche tramite un algoritmo di apprendimento automatico, addestrato su un set di dati, che indica una pluralità di modifiche e un identificativo di un'entità che ha eseguito ciascuna della pluralità di modifiche.

[0018] In alcuni esempi, il metodo può comprendere il recupero, per la prima istantanea e la seconda istantanea, di metadati che indicano stati del dispositivo di calcolo nel primo tempo e nel secondo tempo. Il metodo può comprendere la determinazione di un primo punteggio delle prestazioni basato su uno stato del dispositivo di calcolo nel primo tempo e di un secondo punteggio delle prestazioni basato su uno stato del dispositivo di calcolo nel secondo tempo. Il metodo può comprendere la determinazione di un differenziale di modifica tra il primo punteggio delle prestazioni e il secondo punteggio delle prestazioni, e il contrassegno di un punto nel tempo nella mappa delle modifiche se il differenziale di modifica è superiore a un differenziale di modifica di soglia.

[0019] Va notato che il metodo sopra descritto potrebbero essere implementati in un sistema comprendente un processore hardware.

[0020] Il suddetto compendio semplificato di aspetti esemplificativi serve a fornire una conoscenza di base della presente divulgazione. Il presente compendio non è una panoramica esaustiva di tutti gli esempi contemplati e non è destinato a identificare elementi chiave o fondamentali di tutti gli esempi, né a delineare il campo di applicazione di uno o di tutti gli esempi della presente divulgazione. Il suo unico scopo è presentare uno o più esempi in forma semplificata in vista della descrizione più dettagliata della divulgazione di seguito riportata. Per raggiungere tale obiettivo, l'esempio o gli esempi di cui alla presente divulgazione includono le caratteristiche descritte e specificate a titolo esemplificativo nelle rivendicazioni.

BREVE DESCRIZIONE DEI DISEGNI

[0021] I disegni accompagnatori, che sono acclusi e costituiscono parte integrante delle presenti specifiche, illustrano uno o più aspetti esemplificativi della presente divulgazione e, insieme alla descrizione dettagliata, servono a spiegare i rispettivi principi e le rispettive implementazioni.

La FIG. 1 è un diagramma a blocchi illustrante un sistema per riferimento incrociato di istantanee forensi nel tempo.

La FIG. 2 è un diagramma a blocchi illustrante un'interfaccia utente che evidenzia punti nel tempo di interesse per l'analisi forense.

La FIG. 3 è un diagramma a blocchi che illustra un'interfaccia utente in cui un file viene selezionato per un'analisi di approfondimento (drill-down).

La FIG. 4 illustra un diagramma di flusso di un metodo per il riferimento incrociato di istantanee forensi nel tempo.

La FIG. 5 presenta un esempio di un sistema informatico a uso generale, su cui possono essere implementati esempi della presente divulgazione.

DESCRIZIONE DETTAGLIATA

[0022] Nel presente documento sono descritti aspetti esemplificativi nel contesto di un metodo per il riferimento incrociato di istantanee forensi nel tempo. Agli esperti del settore risulta chiaro che la seguente descrizione è puramente illustrativa e non è destinata a essere in alcun modo limitativa. Altri esempi si suggeriranno prontamente agli esperti del settore che trarranno beneficio dalla presente divulgazione. A questo punto verrà fatto riferimento in dettaglio alle implementazioni degli aspetti esemplificativi illustrati nei disegni accompagnatori. Gli stessi indicatori di riferimento saranno utilizzati nella misura possibile in tutti i disegni e nella successiva descrizione in riferimento agli stessi elementi o a elementi simili.

[0023] Per ovviare alle lacune descritte nell'antefatto, la presente divulgazione confronta il backup e il dump della memoria in più istantanee di backup, per identificare elementi sospetti e modifiche del file di sistema (ad es. file di configurazione e processi che sono cambiati nel corso di più istantanee). Un sistema esemplificativo crea quindi una mappa delle modifiche che viene aggiornata ogniqualvolta viene creato un nuovo backup. Tale mappa delle modifiche funge da struttura portante per un'interfaccia utente (IU) della Time Machine forense, che viene fornita all'investigatore forense. Questa IU consente all'investigatore di effettuare riferimenti incrociati di istantanee forensi in vari punti nel tempo (ad es. esplorare

modifiche critiche definite dall'utente o da un algoritmo di apprendimento automatico) e consente di eseguire un'analisi di approfondimento (drill-down).

[0024] La FIG. 1 è un diagramma a blocchi che illustra un sistema 100 per riferimenti incrociati di istantanee forensi nel tempo. Nel sistema 100, il dispositivo di calcolo 102 può essere un computer, laptop, smartphone, server o qualsiasi altro dispositivo in grado di memorizzare dati che vengono sottoposti a backup. Il dispositivo di calcolo 102 può generare periodicamente istantanee (ad es. backup dei dati e/o dump della memoria) come l'istantanea 104. In alcuni esempi, l'istantanea 104 è un backup dell'immagine del dispositivo di calcolo 102. In altri esempi, l'istantanea 104 è una raccolta di file, processi, applicazioni ecc. che vengono memorizzati su un dispositivo di calcolo 102. L'istantanea 104 può essere salvata su un dispositivo di calcolo 102, oppure può essere trasmessa a un server remoto a cui è collegato detto dispositivo di calcolo 102.

[0025] Nella presente divulgazione, il componente forense 106 è configurato per analizzare le istantanee prodotte dal dispositivo di calcolo 102 e generare una mappa delle modifiche che consenta a qualsiasi investigatore forense, amministratore del dispositivo e utente del dispositivo di effettuare riferimenti incrociati di istantanee su una pluralità di punti nel tempo. Questo inserimento di riferimenti incrociati consente di eseguire l'analisi forense in modo efficiente, organizzato e mirato. Il componente forense 106 può essere salvato sul dispositivo di calcolo 102, oppure può essere suddiviso tra il dispositivo di calcolo 102 e un server remoto in uno schema thin client e thick client. Ad esempio, il dispositivo di calcolo 102 può trasmettere l'istantanea 104 al server remoto in cui è installato il componente forense 106. Il componente forense 106 sul server remoto può creare una mappa delle modifiche attraverso più istantanee ricevute e trasmettere la mappa delle modifiche a un thin client del componente forense 106 sul dispositivo di calcolo 102. Il thin client può quindi presentare la mappa delle modifiche sul dispositivo di calcolo 102.

[0026] Il componente forense 106 comprende un filtro istantanee 108, che identifica specifici file nelle istantanee necessarie per il confronto, il differenziatore 110, che è un modulo che confronta le istantanee filtrate, e un generatore di mappe delle modifiche 112, che è un modulo che crea una mappa delle modifiche con informazioni sulle istantanee in vari punti del tempo che possono essere visualizzati. In alcuni esempi, il componente forense 106 può essere un componente di un software di sicurezza (ad es. un'applicazione anti-virus) o un software di backup. In altri esempi, il componente forense 106 può essere un'applicazione standalone.

[0027] Più nello specifico, il componente forense 106 può ricevere una prima istantanea (ad es. l'istantanea 104) di un dispositivo di calcolo (ad es. il dispositivo di calcolo 102) in un primo tempo (ad es. t1) e una seconda istantanea (ad es. l'istantanea 105) del dispositivo di calcolo in un secondo tempo (ad es. t2). Il componente forense 106 può quindi applicare un filtro predefinito (ad es. il filtro dell'istantanea 108) alla prima istantanea e alla seconda istantanea. Il filtro predefinito include un elenco di file che devono essere estratti da ogni istantanea. Ad esempio, il filtro predefinito può escludere l'estrazione di file di cache.

[0028] Successivamente all'applicazione del filtro predefinito, il componente forense 106 identifica, tramite il differenziatore 110, eventuali differenze nell'elenco dei file estratti dalla prima istantanea e dalla seconda istantanea. Il componente forense 106 crea, tramite un generatore della mappa delle modifiche 112, una mappa delle modifiche (ad es. la mappa 116) per il dispositivo di calcolo che comprende le differenze nell'elenco dei file e dei processi nel corso di un periodo di tempo (il quale periodo di tempo comprende il primo tempo e il secondo tempo). Il componente forense 106 può quindi emettere la mappa delle modifiche in un'interfaccia utente (ad es., UI 114).

[0029] In alcuni esempi, man mano che vengono generate nuove istantanee, il componente forense 106 potrebbe aggiornare dinamicamente la mappa delle modifiche. Ad esempio, il componente forense 106 può ricevere una terza istantanea del dispositivo di calcolo (ad es. dispositivo di calcolo 102) in un terzo tempo (ad es. t3). Il componente forense 106 può quindi applicare il filtro predefinito (ad es. il filtro istantanee 108) alla terza istantanea e identificare eventuali differenze nell'elenco di file estratti dalla seconda istantanea e dalla terza istantanea. In base alle modifiche identificate, il componente forense 106 può modificare la mappa delle modifiche (ad es. 116) per il dispositivo di calcolo in modo da includere inoltre eventuali differenze nell'elenco dei file nel terzo tempo (ad es. t3).

[0030] In termini di aspetto della mappa delle modifiche, la mappa delle modifiche (ad es. la mappa 116) viene emessa visivamente in un'interfaccia utente (ad es. IU 114) come una sequenza temporale con una pluralità di punti nel tempo selezionabili 118, ciascuno dei quali rappresenta un'istantanea del dispositivo di calcolo. Il componente forense 106 può pertanto ricevere una selezione di un punto nel tempo (ad es. punto nel tempo selezionato 120) e generare una finestra con rispettive differenze tra un'istantanea filtrata, associata al punto nel tempo, e una precedente istantanea filtrata. In riferimento al sistema 100, il punto nel tempo selezionato può essere il punto nel tempo t2, ovvero il momento in cui è stata acquisita la seconda istantanea. Di conseguenza, la finestra 122 presenta le differenze nell'elenco dei file estratti dalla prima istantanea e dalla seconda istantanea (ad es. in che modo il dispositivo di calcolo 102 cambia tra tempo t1 e t2). In alcuni esempi, la finestra 122 è interattiva e presenta un'analisi di approfondimento (drill-down) per ogni file nelle rispettive differenze. Ad esempio, se la finestra 122 indica che il file 1 è cambiato tra t1 e t2, un utente può selezionare un identificativo del file 1 (ad es. l'icona di un'applicazione) per ricevere informazioni riguardo a causa della modifica, ora della modifica, registri di accesso, dipendenze ecc. In alcuni esempi, uno stato del file 1 può essere presentato tramite la finestra 122. In alcuni esempi, i file possono essere precaricati nella finestra 122. Va notato che, sebbene nella presente divulgazione vengano citati principalmente file, nella presentazione delle istantanee vengono considerati anche i processi.

[0031] In alcuni esempi, il componente forense 106 può emettere l'IU 114 sul dispositivo di calcolo 102 e/o un dispositivo di analisi di un organo di indagine forense in risposta al rilevamento di un errore nel dispositivo di calcolo 102. Ad esempio, il componente forense 106 può essere installato su un server remoto come thick client che riceve informazioni da un thin client del componente forense 106. Il thick client può monitorare messaggi periodici di heartbeat dal thin client. In risposta alla determinazione del fatto che un periodo soglia di tempo (ad es. un'ora) sia stato superato senza ricevere alcun messaggio, il componente forense 106 può stabilire che il dispositivo di calcolo 102 abbia subito un arresto anomalo o sia stato compromesso (ad es. tramite ransomware che crittografa dati su dispositivi di calcolo). In alcuni esempi, il componente forense 106 può trasmettere un avviso a un organo di indagine forense, il quale avviso comprende l'accesso alla mappa delle modifiche. Ad esempio, il componente forense 106 può inviare un link alla mappa delle modifiche all'organo di indagine forense tramite Internet (ad es. un URL). Facendo clic sul link si accede all'IU 114.

[0032] La FIG. 2 è un diagramma a blocchi che illustra un'interfaccia utente 200 che evidenzia punti nel tempo di interesse per un'analisi forense. Un obiettivo della presente divulgazione è semplificare i dati presentati per un investigatore forense. In alcuni casi, possono esservi più punti nel tempo e backup associati da visualizzare in una determinata mappa delle modifiche - sovraccaricando un utente. Il componente forense 106 può essere configurato per adattare l'interfaccia utente 200 in modo da evidenziare punti nel tempo di specifico interesse. Pertanto, qualsiasi software dannoso viene immediatamente identificato, analizzato e gestito.

[0033] Ad esempio, in alcuni esempi, il componente forense 106 può adattare la mappa delle modifiche in modo che indichi eventuali modifiche effettuate dall'utente ed eventuali modifiche effettuate da un soggetto non autorizzato. In alcuni esempi, il componente forense 106 può filtrare la mappa delle modifiche per non mostrare le modifiche apportate dall'utente (ad es. modifiche manuali). Ad esempio, il componente forense 106 può classificare ogni modifica nella mappa delle modifiche tramite un algoritmo di apprendimento automatico addestrato su un set di dati che indica una pluralità di modifiche e un identificativo di un'entità che ha eseguito ciascuna della pluralità di modifiche. Il set di dati, nello specifico, può acquisire modifiche che sono state eseguite da un noto soggetto dannoso (ad es. un virus) e classificarle come pericolose. Di conseguenza, se tali modifiche non vengono rilevate, eventuali modifiche rimanenti potrebbero con probabilità essere state eseguite dall'utente. Ad esempio, l'algoritmo di apprendimento automatico può essere una macchina a vettori di supporto monoclasse che viene addestrata con un set di dati che include un esempio, in cui un determinato file viene crittografato in una determinata directory da un software dannoso. Se tale modifica viene rilevata (ad es. corrisponde alla modifica di un input), il componente forense 106 determina che la modifica dell'input viene eseguita da un software dannoso. Tuttavia, se la modifica dell'input è differente, la modifica dell'input viene attribuita all'utente.

[0034] In altri esempi, il componente forense 106 può adeguare l'interfaccia utente 200 in base alle modifiche alle prestazioni del dispositivo di calcolo 102. Ad esempio, il componente forense 106 può identificare quando le prestazioni del dispositivo di calcolo 102 si sono degradate maggiormente e adeguare l'aspetto visivo dei punti nel tempo più vicini sulla mappa delle modifiche 202. Nella FIG. 2, sono illustrati più punti nel tempo e le rispettive modifiche associate. In ogni punto nel tempo, il componente forense 106 determina un punteggio di prestazioni del dispositivo di calcolo 102. Al tempo t1, il punteggio delle prestazioni è 99. Al tempo t2, il punteggio delle prestazioni è 95. La modifica delle prestazioni è -4. Le modifiche nei primi due punti nel tempo, incluso il punto 204, sono rappresentate da icone di una prima dimensione. Al tempo t3, il punteggio delle prestazioni scende a 65. La modifica tra t2 e t3 è -30. Di conseguenza, l'indicatore visivo del punto 206 è di dimensioni maggiori per indicare che l'utente (ad es. l'investigatore forense) dovrebbe concentrarsi sul punto 206. In alcuni esempi, le dimensioni di un indicatore visivo sono proporzionali alla modifica del punteggio delle prestazioni. Ad esempio, le dimensioni dell'indicatore visivo del punto 208 sono superiori rispetto a quelle dell'indicatore visivo del punto 206 e inferiori rispetto a quelle dell'indicatore visivo del punto 204. In altri esempi, possono esservi dimensioni predefinite degli indicatori visivi e il componente forense 106 può fare affidamento su una soglia per stabilire come dimensionare l'indicatore visivo. Ad esempio, una prima soglia potrebbe essere 25 e una seconda soglia potrebbe essere 50 e il componente forense 106 potrebbe confrontare la modifica del punteggio delle prestazioni con ogni soglia. Se la modifica del punteggio delle prestazioni è superiore a una prima soglia, le dimensioni sono impostate su una prima dimensione (ad es. 50 pixel per 50 pixel). Se la modifica del punteggio delle prestazioni è superiore rispetto alla seconda soglia, le dimensioni sono impostate su una seconda dimensione (ad es. 100 pixel per 100 pixel).

[0035] Per due istantanee qualsiasi, il componente forense 106 può ricavare, per la prima istantanea e la seconda istantanea, metadati che indicano stati del dispositivo di calcolo nel primo tempo e nel secondo tempo. Il componente forense 106 può quindi determinare un primo punteggio delle prestazioni in base a uno stato del dispositivo di calcolo nel primo tempo e un secondo punteggio delle prestazioni in base a uno stato del dispositivo di calcolo nel secondo tempo. Il componente forense 106 può determinare un differenziale di modifica tra il primo punteggio delle prestazioni e il secondo punteggio delle prestazioni, e contrassegnare un punto nel tempo (ad es. con un indicatore speciale come una stella o con un cambiamento di dimensioni dell'indicatore visivo) nella mappa delle modifiche se il differenziale di modifica è superiore a un differenziale di modifica di soglia.

[0036] Come accennato in precedenza, le prestazioni possono essere quantificate in base a uno stato del dispositivo di calcolo, il quale stato include una combinazione di attributi quali l'utilizzo medio della CPU, l'utilizzo medio della memoria, la durata di vita della batteria (ad es. se un dispositivo di calcolo è portatile), un numero di crash di applicazioni entro un periodo di tempo (ad es. tra due o più istantanee), un numero di crash del dispositivo di calcolo entro un periodo di tempo, una latenza nell'accedere ad applicazioni/file sul dispositivo di calcolo rispetto al tempo di accesso normale, temperature

dell'hardware del dispositivo di calcolo ecc. Ad esempio, se il componente forense 106 sta determinando le prestazioni sulla base dell'utilizzo medio della CPU (ad es. 86%) e del numero di crash dell'applicazione entro il periodo di tempo (ad es. 4 crash di 10 applicazioni utilizzate in 24 ore), il componente forense 106 può eseguire una combinazione lineare dei valori per determinare un punteggio delle prestazioni. Per semplicità, supponiamo che la combinazione lineare ponga pesi uguali (1) su ogni attributo e sia una media dei due valori. In questo caso, il 14% della CPU è libera e 6 applicazioni su 10 non sono andate in crash. Il punteggio delle prestazioni sarà (14 + 60)/2 = 37. In altri esempi, può essere attribuito un peso superiore a uno degli attributi. Ad esempio, il numero di crash può essere impostato su un peso di 1.1. Il punteggio delle prestazioni sarà pertanto (14 + 1.1*60)/2 = 40.

[0037] Per calcolare il differenziale di modifica delle prestazioni, il componente forense 106 può determinare una pluralità di punteggi delle prestazioni, come descritto in precedenza, su un periodo di tempo. Il componente forense 106 può quindi determinare una pendenza dei punteggi sul periodo di tempo. Ad esempio, se il punteggio delle prestazioni nel tempo t2 è 95 e quindi nel tempo t3 il punteggio delle prestazioni è 65, il differenziale di modifica è -30. Supponiamo che il differenziale di modifica di soglia sia 20. Dato che la grandezza del differenziale di modifica è 30, che è superiore alla soglia, il componente forense 106 può contrassegnare l'indicatore visivo del punto 206 (ad es. contrassegnando le dimensioni dell'indicatore visivo superiori rispetto agli altri indicatori visivi).

[0038] La FIG. 3 è un diagramma a blocchi che illustra l'interfaccia utente 300 in cui un file viene selezionato per l'analisi di approfondimento (drill-down). Supponiamo che un utente selezioni uno degli indicatori visivi di un punto nel tempo nell'interfaccia utente 300. La selezione può lanciare una finestra nell'interfaccia utente che elenchi tutti i file che sono variati tra il punto nel tempo selezionato e un punto nel tempo precedente (ad es. un punto nel tempo immediatamente precedente o un punto del tempo ancora più antecedente nel passato, come il primo punto nel tempo). Ad esempio, l'interfaccia utente può essere una tabella che elenca file e descrive le modifiche (ad es. modifica delle dimensioni, cancellazione, aggiunta, variazione della posizione ecc.) eseguite sul file.

[0039] In alcuni esempi, un utente può selezionare un file specifico ed eseguire un'analisi di approfondimento (drill-down). Un'analisi di approfondimento (drill-down) implica la generazione di una mappa di modifiche specifiche per il file. Ad esempio, sull'interfaccia utente, un utente può selezionare un file specifico e il componente forense 106 può generare una mappa delle modifiche che elenca tutte le modifiche a cui il file è stato sottoposto. Nell'interfaccia utente 300, sono illustrati i tempi t1-t6. Supponiamo che l'utente volesse saperne di più sul File XYZ. Quando l'utente seleziona il file dalla pluralità di icone dei file, viene generata una mappa delle modifiche specifiche del file da parte del componente forense 106. La mappa delle modifiche indica che nel tempo t1, il file è stato creato. Viene inoltre generato un indicatore visivo con i metadati del file (ad es. nome, estensione, applicazione, dimensioni ecc.). Ai tempi t2, t3, t4, non è stata apportata nessuna modifica. Di conseguenza, è elencato il tag „NC" o „No Change" (nessuna modifica). Al tempo t5, il file è stato modificato e le dimensioni del file sono cambiate. In alcuni esempi, la mappa delle modifiche specifiche del file può inoltre mostrare le modifiche che hanno causato il cambiamento di dimensioni del file (ad es. testo aggiunto al documento). Ad esempio, può essere generata un'anteprima del file illustrante il testo supplementare sotto forma di una linea rossa. Al tempo t6, la directory del file è cambiata da cartella „key" a cartella „lock."

[0040] La FIG. 4 illustra un diagramma di flusso del metodo 400 per il riferimento incrociato di istantanee forensi nel tempo. Al punto 402, il componente forense 106 riceve una prima istantanea del dispositivo di calcolo 102 in un primo tempo e una seconda istantanea del dispositivo di calcolo 102 in un secondo tempo. Al 404, il componente forense 106 applica un filtro predefinito (ad es. filtro istantanee 108) alla prima istantanea e alla seconda istantanea, il quale filtro predefinito include un elenco di file che devono essere estratti da ogni istantanea (ad es. ai fini del confronto). Successivamente all'applicazione di un filtro predefinito, al 206, il differenziatore 110 identifica differenze nell'elenco dei file estratti dalla prima istantanea e dalla seconda istantanea. Al 408, il generatore di mappe delle modifiche 112 crea una mappa delle modifiche per il dispositivo di calcolo 102 che comprende le differenze nell'elenco dei file per un periodo di tempo, il quale periodo di tempo comprende il primo tempo e il secondo tempo. Al 410, il componente forense 106 emette la mappa delle modifiche (ad es. la mappa 116) in un'interfaccia utente (ad es. IU 114).

[0041] La FIG. 5 è un diagramma a blocchi che illustra un sistema informatico 20 su cui possono essere implementati esempi di del metodo per il riferimento incrociato di istantanee forensi nel tempo in conformità a un aspetto esemplificativo. Il sistema informatico 20 può essere sotto forma di dispositivi di calcolo multipli oppure sotto forma di un dispositivo di calcolo unico, ad esempio un computer desktop, un notebook, un computer portatile, un dispositivo informatico mobile, uno smartphone, un tablet, un server, un mainframe, un dispositivo incorporato o altre forme di dispositivi informatici.

[0042] Come illustrato, il sistema informatico 20 include un'unità di elaborazione centrale (CPU) 21, una memoria di sistema 22 e un bus di sistema 23 che collega i vari componenti del sistema, inclusa la memoria associata all'unità di elaborazione centrale 21. Il bus di sistema 23 potrebbe comprendere una memoria bus o un controller della memoria bus, un bus periferico e un bus locale che è in grado di interagire con qualsiasi altra architettura bus. Esempi dei bus potrebbero includere PCI, ISA, PCI-Express, HyperTransport™, InfiniBand™, Serial ATA, I^2C e altre interconnessioni idonee. L'unità di elaborazione centrale 21 (denominata anche processore) può includere uno o più insiemi di processori dotati di core singoli o multipli. Il processore 21 potrebbe eseguire uno o più codici eseguibili da computer, implementando le tecniche della presente divulgazione. Ad esempio, eventuali comandi/passaggi discussi nelle FIG. 1-4 possono essere eseguiti dal processore 21. La memoria di sistema 22 potrebbe essere qualsiasi memoria per l'archiviazione dei dati utilizzati e/o programmi informatici che sono eseguibili dal processore 21. La memoria di sistema 22 potrebbe includere memoria

volatile come una memoria ad accesso casuale (RAM) 25 e memoria non volatile come la memoria di sola lettura (ROM) 24, memoria flash ecc. o qualsiasi combinazione delle medesime. Il sistema di ingresso/uscita di base (BIOS) 26 potrebbe archiviare le procedure di base per il trasferimento di informazioni tra elementi del sistema informatico 20, come quelle al momento del caricamento del sistema operativo con l'utilizzo della ROM 24.

[0043] Il sistema informatico 20 potrebbe includere uno o più dispositivi di archiviazione come uno o più dispositivi di archiviazione rimovibili 27, uno o più dispositivi di archiviazione non rimovibili 28, o una combinazione dei medesimi. Uno o più dispositivi di archiviazione rimovibili 27 e dispositivi di archiviazione non rimovibili 28 sono collegati al bus di sistema 23 tramite un'interfaccia di archiviazione 32. In un esempio, i dispositivi di archiviazione e i corrispondenti supporti di archiviazione leggibili da computer sono moduli indipendenti dall'alimentazione elettrica per la memorizzazione di istruzioni del computer, strutture di dati, moduli di programma e altri dati del sistema informatico 20. La memoria di sistema 22, i dispositivi di archiviazione rimovibili 27 e i dispositivi di archiviazione non rimovibili 28 potrebbero utilizzare una varietà di supporti di archiviazione leggibili da computer. Esempi di supporti di archiviazione leggibili da computer includono memoria della macchina, come cache, SRAM, DRAM, zero capacitor RAM, twin transistor RAM, eDRAM, EDO RAM, DDR RAM, EEPROM, NRAM, RRAM, SONOS, PRAM; memoria flash o altra tecnologia di memorizzazione come unità a stato solido (SSD) o unità flash; cassette magnetiche, nastro magnetico e archiviazione su disco magnetico come unità di disco rigido o floppy disc; archiviazione ottica come in compact disc (CD-ROM) o dischi versatili digitali (DVDs); e qualsiasi altro supporto che possa essere utilizzato per archiviare i dati desiderati e a cui sia possibile accedere tramite il sistema informatico 20.

[0044] La memoria di sistema 22, i dispositivi di archiviazione rimovibili 27 e i dispositivi di archiviazione non rimovibili 28 del sistema informatico 20 potrebbero essere utilizzati per archiviare un sistema operativo 35, ulteriori applicazioni del programma 37, altri moduli del programma 38 e dati del programma 39. Il sistema informatico 20 potrebbe includere un'interfaccia periferica 46 per la comunicazione dei dati da dispositivi di input 40, come tastiera, mouse, stilo, controller di game, dispositivo di immissione vocale, dispositivo di ingresso touch o altri dispositivi periferici, come una stampante o uno scanner tramite una o più porte I/O, come una porta seriale, una porta parallela, un bus seriale universale (USB) o altra interfaccia periferica. Un dispositivo di visualizzazione 47, come ad esempio uno o più monitor, proiettori o display integrati, potrebbe essere collegato al bus del sistema 23 attraverso un'interfaccia di uscita 48, come un adattatore video. Oltre ai dispositivi di visualizzazione 47, il sistema informatico 20 potrebbe essere dotato di altri dispositivi di uscita periferici (non illustrati), quali altoparlanti e altri dispositivi audiovisivi.

[0045] Il sistema informatico 20 potrebbe operare in un ambiente di rete, utilizzando un collegamento di rete a uno o più computer remoti 49. Il computer remoto (o i computer remoti) 49 potrebbero essere postazioni di lavoro o server informatici locali, comprendenti la maggior parte o tutti i suddetti elementi nel descrivere la natura di un sistema informatico 20. Altri dispositivi potrebbero inoltre essere presenti nella rete informatica, quali ad esempio, non in modo esaustivo, router, stazioni di rete, dispositivi peer o altri nodi di rete. Il sistema informatico 20 potrebbe includere una o più interfacce di rete 51 o adattatori di rete per la comunicazione con i computer remoti 49 tramite una o più reti quali una rete informatica a raggio locale (LAN) 50, una rete informatica ad ampio raggio (WAN), un intranet e Internet. Esempi dell'interfaccia di rete 51 potrebbero includere un'interfaccia Ethernet, un'interfaccia Frame Relay, un'interfaccia SONET e interfacce wireless.

[0046] Esempi della presente divulgazione potrebbero essere un sistema ed un metodo e/o un prodotto di programma informatico. Il prodotto di programma informatico potrebbe includere un supporto (o più supporti) di archiviazione leggibile da computer, dotato di istruzioni di programma leggibili da computer sul medesimo, che porta un processore a eseguire esempi della presente divulgazione.

[0047] Il supporto di archiviazione leggibile da computer può essere un dispositivo tangibile che può conservare e memorizzare il codice del programma sotto forma di istruzioni o strutture di dati accessibili da un processore di un dispositivo di calcolo, come un sistema computerizzato 20. Il supporto di archiviazione leggibile dal computer potrebbe essere un dispositivo di archiviazione elettronico, un dispositivo di archiviazione magnetico, un dispositivo di archiviazione ottico, un dispositivo di archiviazione elettromagnetico, un dispositivo di archiviazione a semiconduttori oppure qualsiasi combinazione idonea dei medesimi. A titolo esemplificativo, tale supporto di archiviazione leggibile da computer può comprendere una memoria ad accesso casuale (RAM), una memoria di sola lettura (ROM), un EEPROM, una memoria di sola lettura a disco compatto portatile (CD-ROM), un disco digitale versatile (DVD), una memoria flash, un disco rigido, un dischetto per computer portatile, un memory stick o perfino un dispositivo codificato meccanicamente come schede perforate o strutture in rilievo in una scanalatura su cui siano registrate istruzioni. Secondo il presente utilizzo, il supporto di archiviazione leggibile dal computer non deve essere inteso come segnali transitori in sé, ad esempio onde radio o altre onde elettromagnetiche a propagazione libera, onde elettromagnetiche propagantisi attraverso una guida d'onda o supporti di trasmissione o segnali elettrici trasmessi via cavo.

[0048] Le istruzioni di programma leggibili da computer qui descritte possono essere scaricate nei rispettivi dispositivi di calcolo da un supporto di memorizzazione leggibile da computer o un computer esterno o un dispositivo di archiviazione esterno tramite una rete, ad esempio Internet, una rete di area locale, una rete ad ampio raggio e/o una rete wireless. La rete potrebbe comprendere cavi di trasmissione in rame, fibre ottiche di trasmissione, trasmissione wireless, router, firewall, interruttori, computer gateway e/o server perimetrali. Un'interfaccia di rete in ogni dispositivo di calcolo riceve istruzioni di programma leggibili da computer a partire dalla rete e inoltra le istruzioni di programma leggibili da computer per l'archiviazione in un supporto di archiviazione leggibile da computer all'interno del rispettivo dispositivo di calcolo.

[0049] Le istruzioni di programma leggibili da computer per l'esecuzione di operazioni della presente divulgazione potrebbero essere istruzioni di assemblaggio, architettura dell'insieme delle istruzioni (ISA), istruzioni macchina, istruzioni dipendenti dalla macchina, microcodice, istruzioni firmware, dati sull'impostazione dello stato o un codice sorgente o codice oggetto scritto in qualsiasi combinazione di una o più linguaggi di programmazione, incluso un linguaggio di programmazione orientato all'oggetto e linguaggi di programmazione procedurali convenzionali. Le istruzioni di programma leggibili da computer potrebbero essere eseguibili interamente sul computer dell'utente, in parte sul computer dell'utente sotto forma di pacchetto software stand-alone, in parte sul computer dell'utente e in parte su un computer remoto o interamente sul computer o server remoto. In quest'ultimo scenario, il computer remoto potrebbe essere collegato al computer dell'utente tramite qualsiasi tipo di rete, ivi inclusa una LAN o WAN, oppure il collegamento potrebbe essere effettuato verso un computer esterno (ad esempio tramite Internet). In alcune forme di realizzazione, la circuitistica elettronica, ivi inclusi, ad esempio, il circuito logico programmabile, gate array programmabili in campo (FPGA) o array logici programmabili (PLA), potrebbe eseguire istruzioni leggibili da computer utilizzando informazioni di stato delle istruzioni di programma leggibili da computer per personalizzare il circuito elettronico al fine di eseguire esempi della presente divulgazione.

[0050] In vari esempi, il sistema e i metodo descritti nella presente divulgazione possono essere indirizzati in termini di moduli. Il termine „modulo“ qui utilizzato si riferisce a un dispositivo del mondo reale, un componente o una disposizione di componenti implementati tramite hardware, ad esempio da un circuito integrato specifico per l'applicazione (ASIC) o FPGA, ad esempio, o come combinazione di hardware e software, ad esempio da un sistema a microprocessore e un insieme di istruzioni per implementare la funzionalità del modulo, che (durante l'esecuzione) trasforma il sistema di microprocessore in un dispositivo per scopi specifici. Un modulo potrebbe inoltre essere implementato come una combinazione dei due, con determinate funzioni facilitate dal solo hardware e altre funzioni facilitate da una combinazione di hardware e software. In determinate implementazioni, almeno una porzione, e in alcuni casi tutte le porzioni, di un modulo potrebbero essere eseguite sul processore di un sistema informatico. Di conseguenza, ogni modulo potrebbe essere realizzato in una varietà di configurazioni idonee e non dovrebbe essere limitato ad alcuna implementazione particolare qui esemplificata.

[0051] Ai fini della chiarezza, non vengono qui divulgate tutte le funzionalità di routine degli esempi. Sarebbe apprezzato che, nello sviluppo di qualsiasi implementazione effettiva della presente divulgazione, venissero prese numerose decisioni per specifiche implementazioni al fine di ottenere gli obiettivi specifici dello sviluppatore e tali obiettivi specifici varieranno per diverse implementazioni e diversi sviluppatori. Resta inteso che tale sforzo di sviluppo potrebbe essere complesso e richiedere tempo ma sarebbe tuttavia un'attività ingegneristica di routine per gli esperti del settore che usufruiscano di questa divulgazione.

[0052] Inoltre, resta inteso che la fraseologia o la terminologia utilizzate in questo contesto sono puramente descrittive e non limitative, per cui la terminologia o fraseologia di cui alle presenti specifiche deve essere interpretata dagli esperti del settore alla luce degli insegnamenti e delle linee guida qui presentate, in combinazione alle conoscenze degli esperti nel rispettivo o nei rispettivi campi. Inoltre, qualunque termine riportato nelle specifiche o nelle rivendicazioni non è da intendersi come attribuibile a un significato insolito o speciale, salvo esplicitamente indicato come tale.

[0053] I vari esempi qui divulgati comprendono equivalenti noti presenti e futuri ai moduli noti, qui riferiti a titolo illustrativo. Inoltre, sebbene siano stati illustrati e descritti esempi e applicazioni, risulta evidente agli esperti del settore che hanno il beneficio di consultare la presente divulgazione, che sono possibili molte più modifiche rispetto a quelle citate in precedenza, senza discostarsi dai concetti inventivi qui divulgati.

Rivendicazioni

1. Metodo per il riferimento incrociato di istantanee forensi nel tempo, il quale metodo comprende:
   ricevere una prima istantanea (104) di un dispositivo di calcolo (102) in un primo tempo (t1) e una seconda istantanea (105) del dispositivo di calcolo (102) in un secondo tempo (t2);
   applicare un filtro predefinito (108) alla prima istantanea (104) e alla seconda istantanea (105), il quale filtro predefinito (108) estrae un elenco dei file da ciascuna di detta pima e seconda istantanea;
   successivamente all'applicazione del filtro predefinito (108), identificare differenze nell'elenco dei file estratti dalla prima istantanea (104) e dalla seconda istantanea (105);
   creare una mappa delle modifiche (112) per il dispositivo di calcolo (102) che comprenda le differenze nell'elenco dei file su un periodo di tempo, il quale periodo di tempo comprenda il primo tempo (t1) e il secondo tempo (t2); e
   emissione, tramite un componente software forense (106) del dispositivo di calcolo (102), della mappa delle modifiche in un'interfaccia utente (114).
2. Metodo secondo la rivendicazione 1, comprendente inoltre:
   ricevere una terza istantanea del dispositivo di calcolo (102) in un terzo tempo (t3);
   applicare il filtro predefinito (108) alla terza istantanea;
   identificare differenze nell'elenco dei file estratti dalla seconda istantanea (104) e dalla terza istantanea;
   modificare la mappa delle modifiche (112) affinché il dispositivo di calcolo (102) includa inoltre differenze nell'elenco dei file sul periodo di tempo, il quale periodo di tempo comprenda anche il terzo tempo (t3).

3. Metodo secondo una delle rivendicazioni da 1 a 2, in cui la mappa delle modifiche (112) viene emessa visivamente nell'interfaccia utente (114) sotto forma di una sequenza temporale con una pluralità di punti nel tempo selezionabili, ciascuno dei quali rappresenta un'istantanea del dispositivo di calcolo, comprendente inoltre:
ricevere la selezione di un punto nel tempo; e
generare una finestra con rispettive differenze tra un'istantanea filtrata associata al punto nel tempo e una precedente istantanea filtrata.

4. Metodo secondo la rivendicazione 3, in cui il punto nel tempo selezionato è il secondo tempo (t2) associato alla seconda istantanea (105) e in cui la finestra presenta le differenze nell'elenco dei file estratti dalla prima istantanea (104) e dalla seconda istantanea (105).

5. Metodo secondo le rivendicazioni da 3 a 4, in cui la finestra è interattiva e presenta un'analisi di approfondimento per ciascun file nelle rispettive differenze.

6. Metodo secondo la rivendicazione 5, in cui l'emissione della mappa delle modifiche (112) comprende inoltre trasmettere un avviso a un organo di investigazione forense, il quale avviso comprende l'accesso alla mappa delle modifiche (112).

7. Metodo secondo una delle rivendicazioni da 1 a 6, comprendente inoltre:
recuperare, per la prima istantanea (104) e la seconda istantanea (105), metadati che indicano stati del dispositivo di calcolo (102) nel primo tempo (t1) e nel secondo tempo (t2);
determinare un primo punteggio delle prestazioni basato su uno stato del dispositivo di calcolo (102) nel primo tempo (t1) e di un secondo punteggio delle prestazioni basato su uno stato del dispositivo di calcolo (102) nel secondo tempo (t2);
determinare un differenziale di modifica tra il primo punteggio delle prestazioni e il secondo punteggio delle prestazioni; e
contrassegnare un punto nel tempo nella mappa delle modifiche (112) se il differenziale di modifica è superiore al differenziale di modifica di soglia.

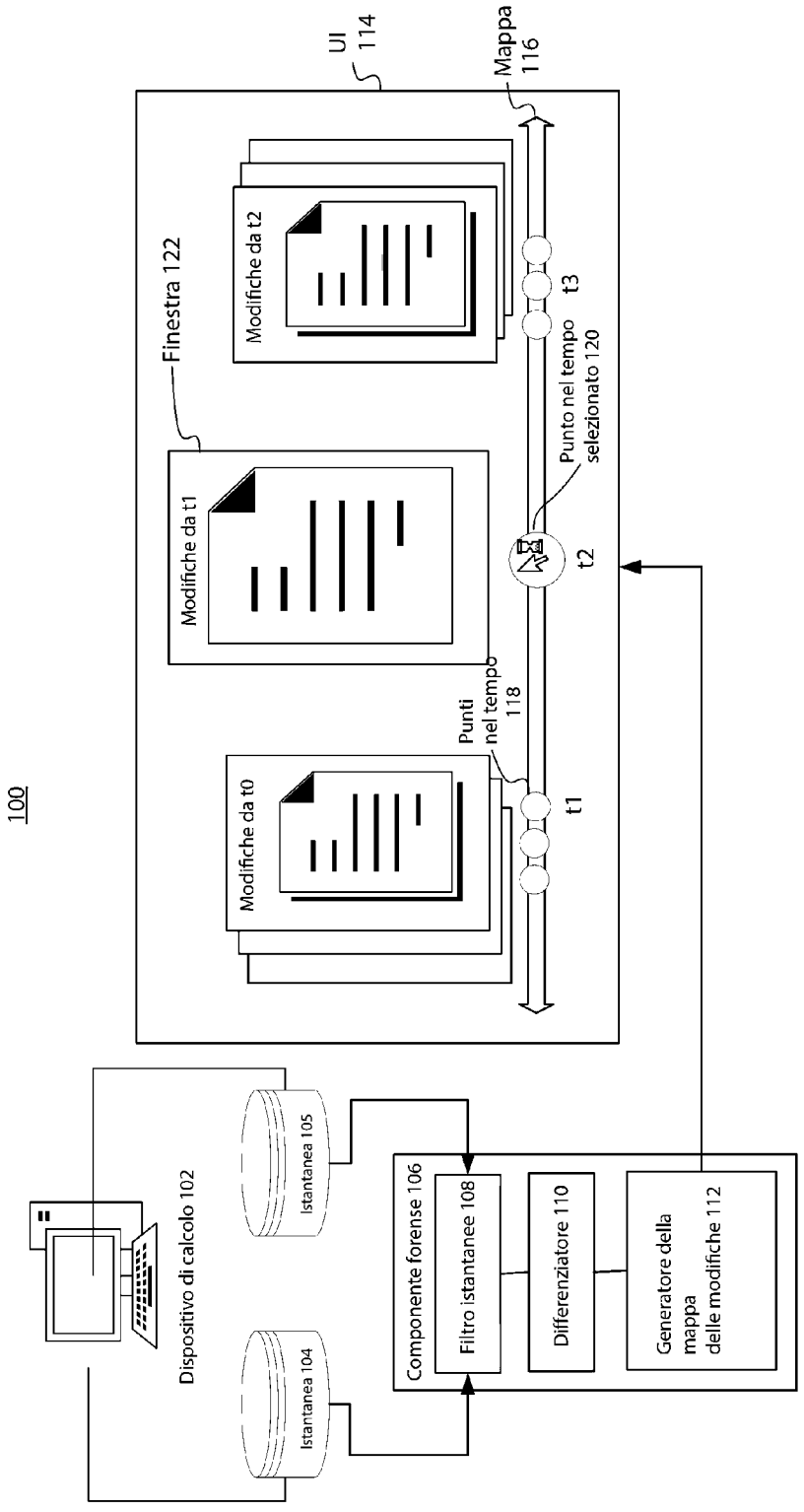

100
UI 114
Mappa 116
Finestra 122
Modifiche da t2
Modifiche da t1
Modifiche da t0
t3
t2
t1
Punto nel tempo selezionato 120
Punti nel tempo 118
Dispositivo di calcolo 102
Istantanea 105
Istantanea 104
Componente forense 106
Filtro istantanee 108
Differenziatore 110
Generatore della mappa delle modifiche 112

FIG 1

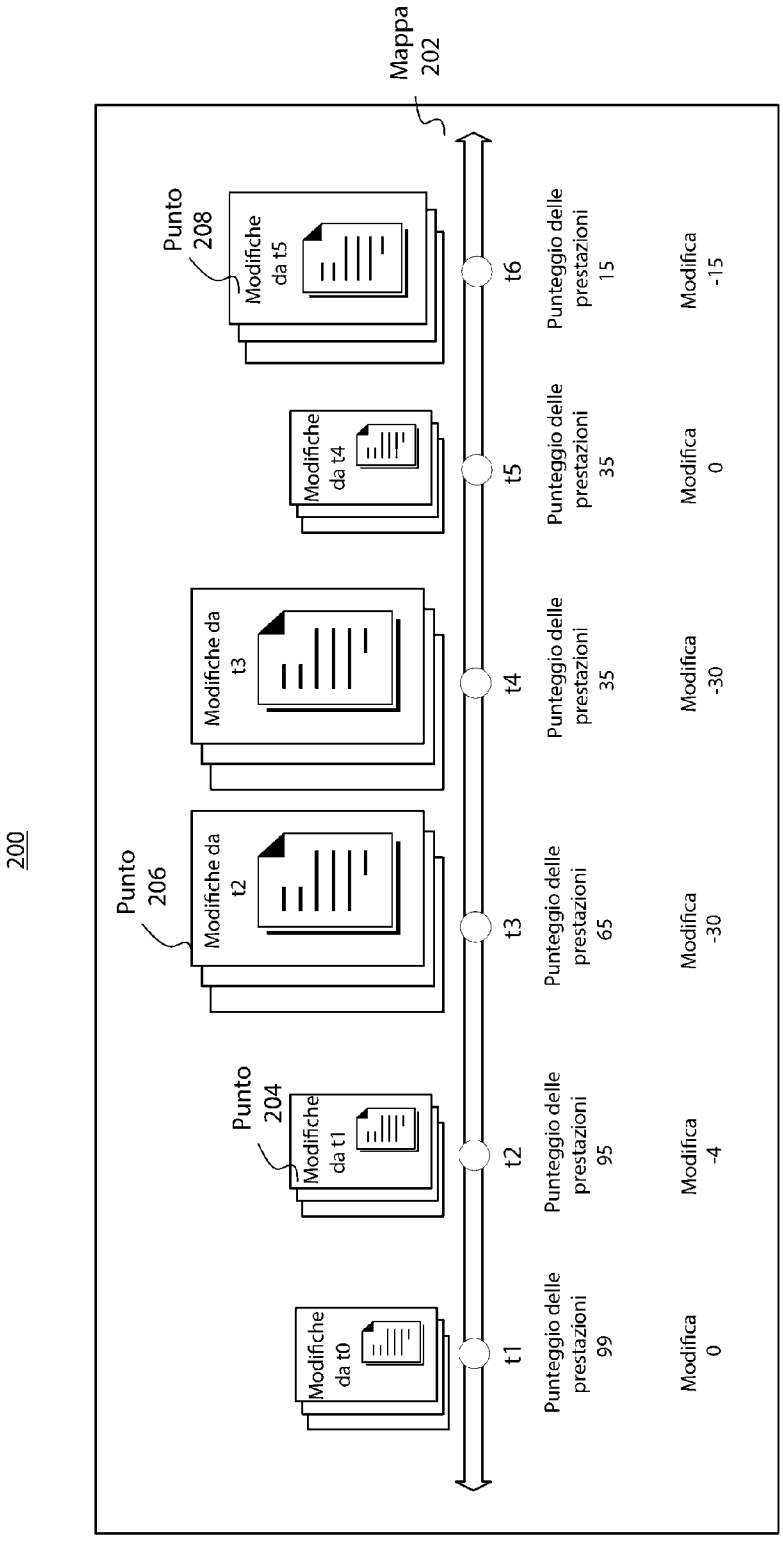

200
Mappa
202
Punto
208
Modifiche
da t5
Punto
206
Modifiche da
t2
Punto
204
Modifiche
da t1
Modifiche
da t0
Modifiche da
t3
Modifiche
da t4
t1
t2
t3
t4
t5
t6
Punteggio delle
prestazioni
99
Punteggio delle
prestazioni
95
Punteggio delle
prestazioni
65
Punteggio delle
prestazioni
35
Punteggio delle
prestazioni
35
Punteggio delle
prestazioni
15
Modifica
0
Modifica
-4
Modifica
-30
Modifica
-30
Modifica
0
Modifica
-15

FIG 2

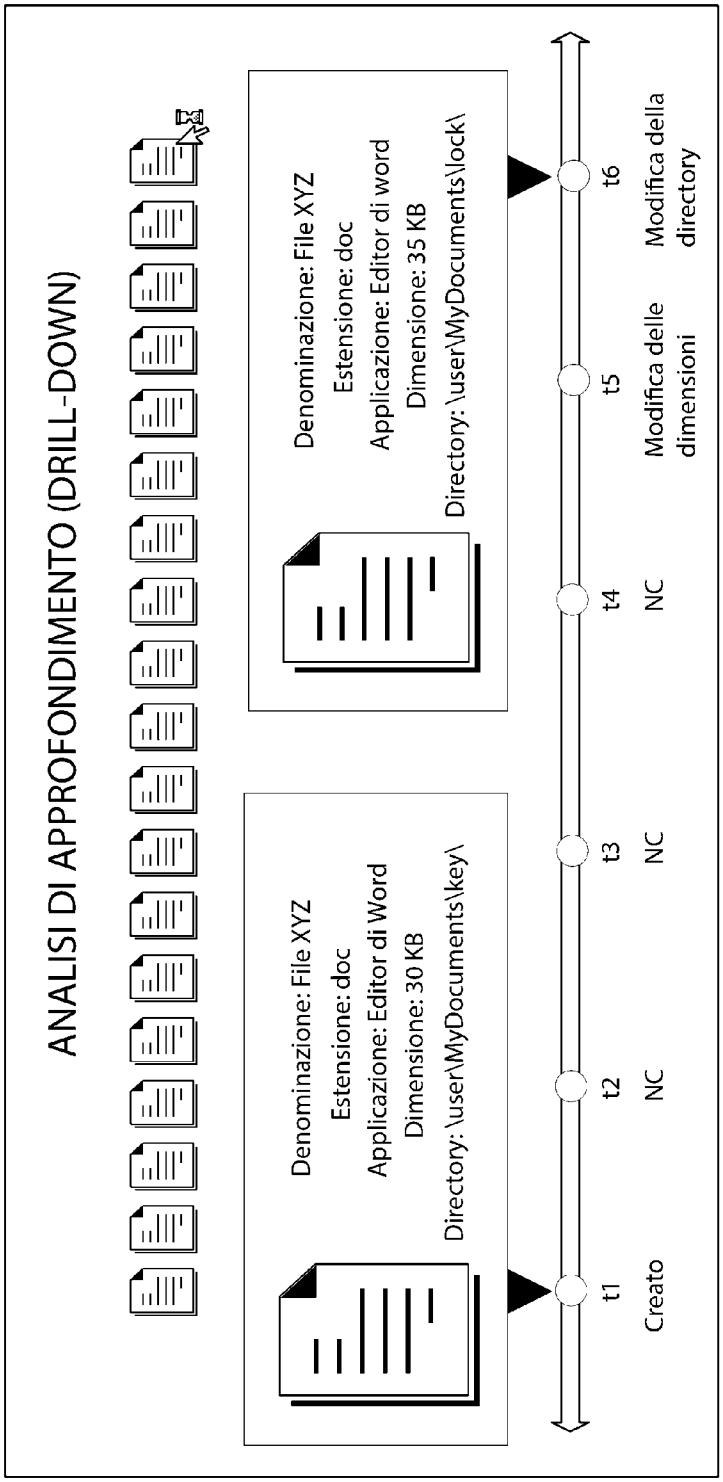

300
ANALISI DI APPROFONDIMENTO (DRILL-DOWN)
Denominazione: File XYZ
Estensione: doc
Applicazione: Editor di Word
Dimensione: 30 KB
Directory: \user\MyDocuments\key\
Denominazione: File XYZ
Estensione: doc
Applicazione: Editor di word
Dimensione: 35 KB
Directory: \user\MyDocuments\lock\
t1
Creato
t2
NC
t3
NC
t4
NC
t5
Modifica delle dimensioni
t6
Modifica della directory

FIG 3

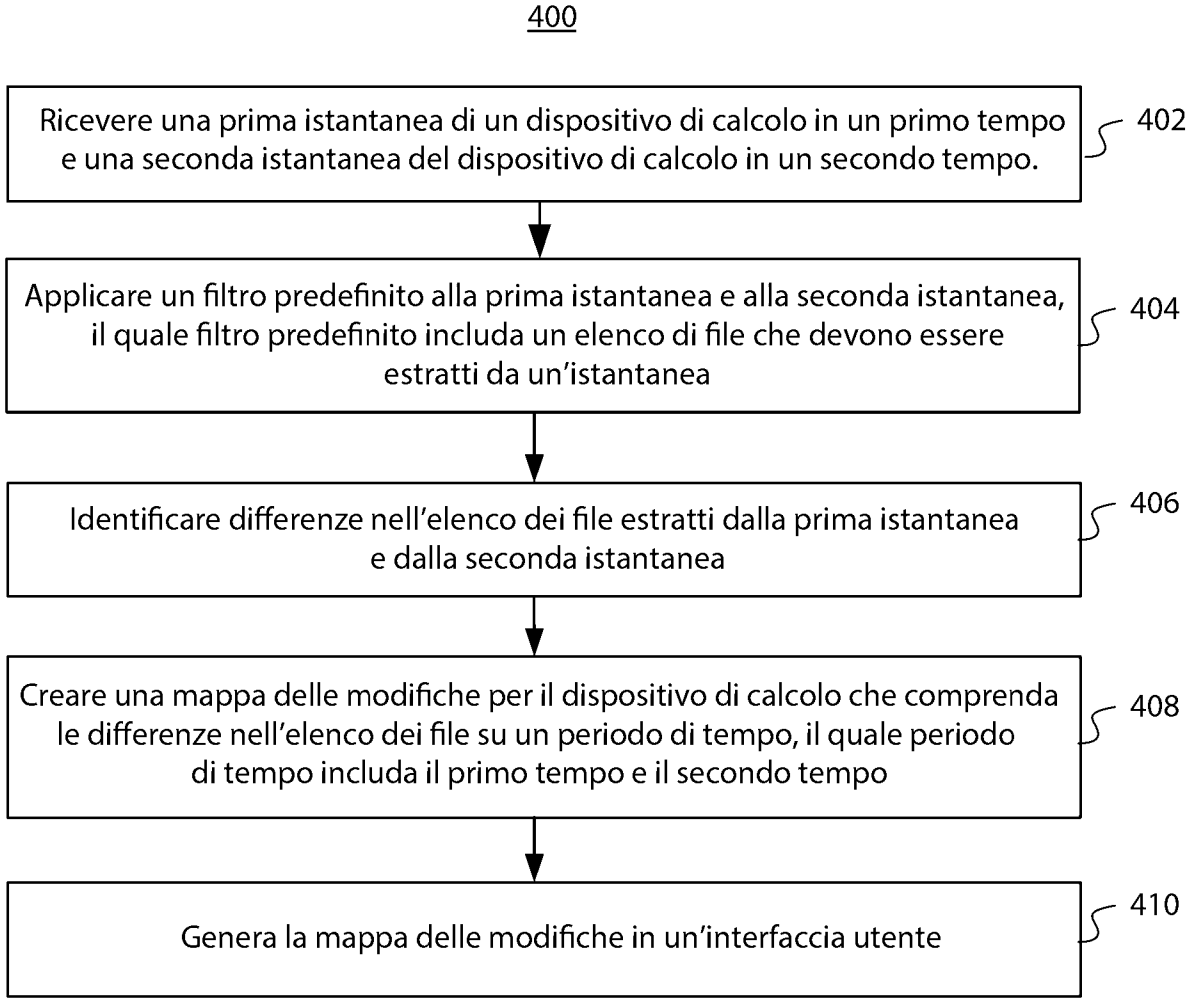

400
Ricevere una prima istantanea di un dispositivo di calcolo in un primo tempo e una seconda istantanea del dispositivo di calcolo in un secondo tempo.
402
Applicare un filtro predefinito alla prima istantanea e alla seconda istantanea, il quale filtro predefinito includa un elenco di file che devono essere estratti da un'istantanea
404
Identificare differenze nell'elenco dei file estratti dalla prima istantanea e dalla seconda istantanea
406
Creare una mappa delle modifiche per il dispositivo di calcolo che comprenda le differenze nell'elenco dei file su un periodo di tempo, il quale periodo di tempo includa il primo tempo e il secondo tempo
408
Genera la mappa delle modifiche in un'interfaccia utente
410

FIG 4

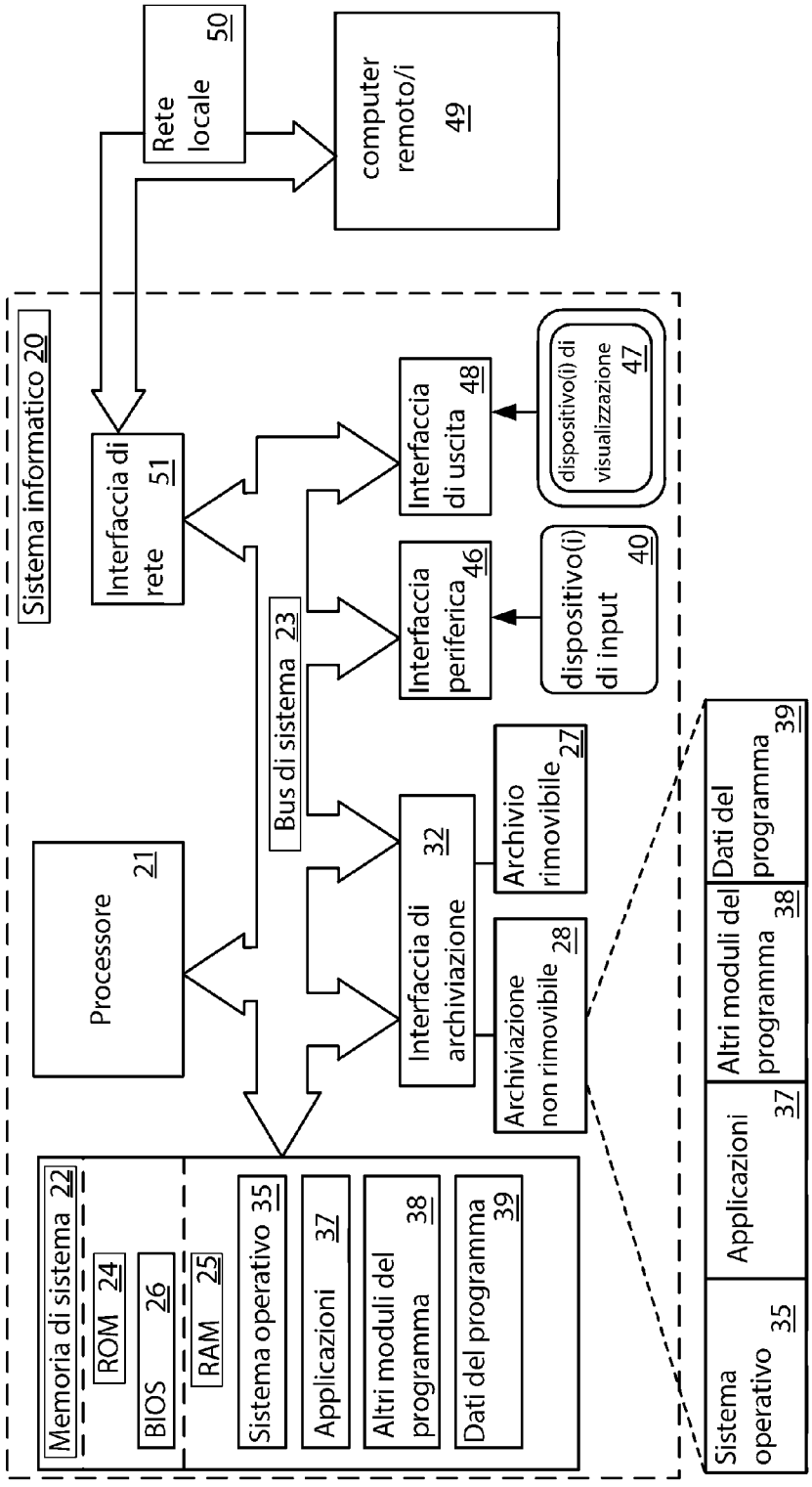

Sistema informatico 20
Memoria di sistema 22
ROM 24
BIOS 26
RAM 25
Sistema operativo 35
Applicazioni 37
Altri moduli del programma 38
Dati del programma 39
Processore 21
Bus di sistema 23
Interfaccia di rete 51
Interfaccia di archiviazione 32
Archiviazione non rimovibile 28
Archivio rimovibile 27
Interfaccia periferica 46
Interfaccia di uscita 48
dispositivo(i) di input 40
dispositivo(i) di visualizzazione 47
Rete locale 50
computer remoto/i 49
Sistema operativo 35
Applicazioni 37
Altri moduli del programma 38
Dati del programma 39

FIG. 5