(19) CONFEDERAZIONE SVIZZERA
ISTITUTO FEDERALE DELLA PROPRIETÀ INTELLETTUALE

(11) **CH 716 656 B1**

(51) Int. Cl.: ***G06F 11/14*** *(2006.01)*
G06F 21/55 *(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: 001317/2019

(22) Data di deposito: 16.10.2019

(43) Domanda pubblicata: 31.03.2021

(30) Priorità: 25.09.2019 US 16/582,497

(24) Brevetto rilasciato: 29.11.2024

(45) Fascicolo del brevetto pubblicato: 29.11.2024

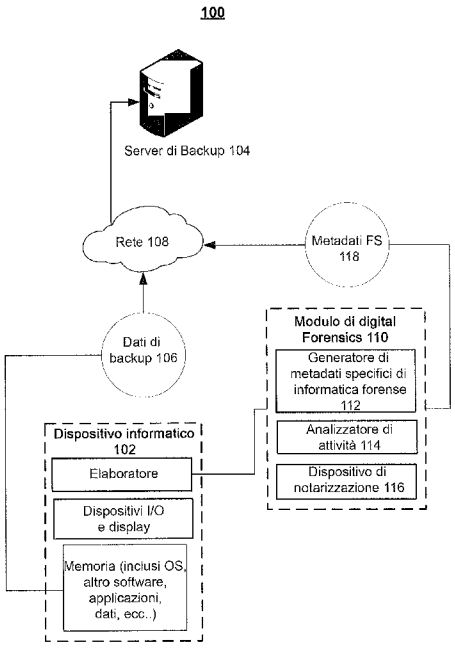
(73) Titolare/Titolari:
Acronis International GmbH, Rheinweg 9
8200 Schaffhausen (CH)

(72) Inventore/Inventori:
Vladimir Strogov, 8200 Schaffhausen (CH)
Oleg Ishanov, 8200 Schaffhausen (CH)
Alexey Dod, 8200 Schaffhausen (CH)
Serguei Beloussov, 8200 Schaffhausen (CH)
Stanislav Protasov, 8200 Schaffhausen (CH)

(74) Mandatario:
Ing. Marco Zardi c/o M. ZARDI & Co. S.A., via Pioda 6
6900 Lugano (CH)

(54) Metodo di generazione e archivazione di metadati specifici dell'informatica forense.

(57) L'invenzione riguarda un metodo ed un sistema, per la generazione e l'archiviazione di metadati specifici dell'informatica forense. In un esempio, un modulo di digital forensics (110) è configurato per generare un backup dei dati utente memorizzati su un dispositivo informatico (102) conformemente a un piano di backup. Il modulo di digital forensics (110) identifica, a partire da una pluralità di metadati di sistema del dispositivo informatico (102), i metadati specifici dell'informatica forense del dispositivo informatico (102) in base a regole predeterminate, in cui i metadati specifici dell'informatica forense sono utilizzati per rilevare attività digitali sospette. Il modulo di digital forensics (110) genera un backup dei metadati specifici dell'informatica forense conformemente al piano di backup e analizza i metadati specifici dell'informatica forense per rilevare un'indicazione dell'attività digitale sospetta sul dispositivo informatico (102). In risposta alla rilevazione dell'attività digitale sospetta sulla base dell'analisi, il sistema genera un evento di sicurezza indicante che l'attività digitale sospetta si è verificata.



Descrizione

CAMPO TECNICO

[0001] La presente esposizione riguarda il settore della sicurezza dei dati e, più specificamente, i sistemi e i metodi di generazione e archiviazione di metadati specifici dell'informatica forense per indagare su attività digitali sospette.

STATO DELL'ARTE

[0002] I dati presenti su un dispositivo informatico possono dover essere ripristinati per vari motivi. Ad esempio, un sistema operativo di un dispositivo informatico può essere danneggiato ed il sistema può aver bisogno di recuperare un insieme non danneggiato di file di backup al posto di quelli danneggiati. Generalmente, le copie di backup sono eseguite unicamente per i dati necessari a ripristinare il sistema di un utente. Questi dati possono includere applicazioni installate, impostazioni, documenti, file, database, ecc.

[0003] Con l'aumento del ricorso all'informatica digitale, la quantità di reati informatici come l'hacking, il furto di dati e gli attacchi di malware, è aumentata di pari passo. Di conseguenza, è necessario salvare informazioni aggiuntive sui dati di un sistema quando si creano copie di backup che possono essere utilizzate per indagare su questi crimini informatici. Gli ingegneri forensi possono utilizzare queste informazioni aggiuntive per stabilire l'origine di un attacco e rilevare i rimanenti artefatti e le tracce dell'attacco su un sistema.

[0004] Tuttavia, le indagini nel campo della digital forensics richiedono urgenza, tempo e manodopera. Un approccio basato sulla forza bruta nell'analisi dei dati elemento per elemento non è efficace perché questo approccio comporta svariati presupposti, come l'autenticità dei dati analizzati e il fatto che oggetti non fidati non vengano cancellati da un malintenzionato. Il tempo necessario per portare a termine un'indagine con questo approccio dipende inoltre dalla quantità di dati da analizzare. Ad esempio, il tempo necessario per la revisione di un disco rigido di grandi dimensioni può essere esponenzialmente maggiore del tempo necessario per un disco rigido più piccolo, perché gli investigatori hanno molti più file da esaminare e non necessariamente potrebbero sapere da dove iniziare l'analisi. Questo approccio può essere ancora più scoraggiante se un'indagine non è conclusiva perché i dati rilevanti di un sistema sono già stati rimossi quando l'investigatore inizia l'analisi perché, ad esempio, il dispositivo informatico in questione è stato riavviato, formattato o danneggiato.

[0005] Vi è quindi la necessità di un metodo per generare e archiviare i metadati specifici dell'informatica forense che affronti le carenze sopra descritte.

SOMMARIO

[0006] La presente invenzione rivendica un metodo per l'archiviazione di metadati specifici dell'informatica forense, secondo la rivendicazione 1.

[0007] Forme di realizzazione preferite del metodo secondo la rivendicazione 1 sono definite nelle rivendicazioni dipendenti da 2 a 10.

[0008] L'esposizione riguarda il settore della sicurezza dei dati. In particolare, l'esposizione descrive un metodo per la generazione e l'archiviazione di metadati specifici dell'informatica forense.

[0009] Il metodo per la generazione e l'archiviazione di metadati specifici dell'informatica forense comprende un modulo di digital forensics configurato per generare un backup dei dati utente memorizzati su un dispositivo informatico secondo un piano di backup. Il modulo di digital forensics identifica, a partire da una pluralità di metadati di sistema del dispositivo informatico, i metadati specifici dell'informatica forense del dispositivo informatico basati su regole predeterminate, in cui i metadati specifici dell'informatica forense sono utilizzati per rilevare attività digitali sospette. Il modulo di digital forensics genera un backup dei metadati specifici dell'informatica forense in conformità con il piano di backup, in cui il backup dei metadati specifici dell'informatica forense è memorizzato separatamente dal backup dei dati utente. Il modulo di digital forensics analizza i metadati specifici dell'informatica forense per rilevare un'indicazione di un'attività digitale sospetta sul dispositivo informatico e in risposta alla rilevazione dell'attività digitale sospetta basata sull'analisi genera un evento di sicurezza che indica che l'attività digitale sospetta si è verificata, l'evento di sicurezza essendo un segnale di allerta.

[0010] In un esempio, il modulo di digital forensics contrassegna ulteriormente i successivi backup dei dati utente del piano di backup come potenzialmente interessati dall'attività digitale sospetta.

[0011] In un esempio, il modulo di digital forensics richiede anche l'esecuzione di un'indagine digitale.

[0012] In un esempio, il modulo di digital forensics ripristina anche il dispositivo informatico con un precedente backup dei dati utente generati prima dell'attività digitale sospetta.

[0013] In un esempio, il modulo di digital forensics aumenta anche la frequenza di generazione dei backup nel piano di backup dei metadati specifici dell'informatica forense.

[0014] In un esempio, i metadati specifici dell'informatica forense comprendono almeno uno tra: un identificatore di un processo in esecuzione, informazioni sull'allocazione della memoria, un identificatore di un thread in esecuzione, infor-

mazioni sui privilegi di sicurezza, informazioni sul registro, un identificatore di un processo nascosto e un percorso di esecuzione automatica sul dispositivo informatico.

[0015] In un esempio, il modulo di digital forensics genera un identificatore di notarizzazione del backup dei metadati specifici dell'informatica forense, in cui l'identificatore di notarizzazione è uno tra: un identificatore di transazione di blockchain, un valore di hash, una firma digitale, o un codice di controllo. Il modulo di digital forensics memorizza quindi l'identificatore di autenticazione con il backup dei metadati specifici dell'informatica forense.

[0016] In un esempio, il modulo di digital forensics analizza i metadati specifici dell'informatica forense per trovare l'indicazione dell'attività digitale sospetta, identificando prima un primo backup dei metadati specifici dell'informatica forense generato in un primo momento e un secondo backup dei metadati specifici dell'informatica forense generato in un secondo momento dopo la prima volta. Il modulo di digital forensics rileva quindi, a partire dai metadati specifici dell'informatica forense, un processo nel secondo backup che non è presente nel primo backup e determina se il processo è fidato. In risposta alla constatazione che il processo non è fidato, il modulo di digital forensics rileva l'indicazione dell'attività digitale sospetta sul dispositivo informatico.

[0017] In un esempio, il modulo di digital forensics determina se il processo è fidato confrontando il processo con una pluralità di processi fidati noti elencati in una struttura di dati e determinando che non esiste alcuna corrispondenza tra il processo e un processo fidato noto nella pluralità di processi fidati noti.

[0018] In un esempio, il modulo di digital forensics identifica anche le caratteristiche dell'attività digitale sospetta e identifica metadati avanzati specifici dell'informatica forense sulla base di tali caratteristiche in cui i metadati avanzati specifici dell'informatica forense comprendono dettagli specifici delle caratteristiche dell'attività digitale sospetta. Il modulo di digital forensics genera quindi dei backup successivi dei metadati avanzati specifici dell'informatica forense (in aggiunta o in alternativa ai metadati originali specifici dell'informatica forense).

[0019] Il sommario semplificato di cui sopra serve a consentire una comprensione basilare della presente esposizione. Questo sommario non è una panoramica esaustiva di tutte le caratteristiche contemplate. Il suo unico scopo è presentare alcune caratteristiche in forma semplificata come preludio alla descrizione più dettagliata dell'esposizione che segue..

BREVE DESCRIZIONE DEI DISEGNI

[0020]

La FIG. 1 è un diagramma a blocchi che illustra un sistema per la generazione e l'archiviazione di metadati specifici dell'informatica forense.

La FIG. 2 illustra un diagramma di flusso di un esempio di metodo per la generazione e l'archiviazione di metadati specifici dell'informatica forense.

La FIG. 3 illustra un diagramma di flusso di un esempio di metodo per rilevare attività digitali sospette.

La FIG. 4 illustra un diagramma di flusso di un esempio di metodo per aggiornare il piano di backup basato sulla rilevazione di attività digitali sospette.

La FIG. 5 presenta un esempio di un sistema informatico generico.

DESCRIZIONE DETTAGLIATA

[0021] E' di seguito descritto un sistema, metodo e prodotto di programma informatico per la generazione e l'archiviazione di metadati specifici dell'informatica forense. Coloro che hanno un'ordinaria competenza nell'arte si renderanno conto che la seguente descrizione è puramente illustrativa e non intende essere in alcun modo limitativa. Si farà ora riferimento in dettaglio alle implementazioni esemplificative come illustrate nei disegni accompagnatori. Gli stessi indicatori di riferimento saranno utilizzati, nei limiti del possibile, in tutti i disegni e nella seguente descrizione per riferirsi agli stessi elementi o ad elementi simili.

[0022] La FIG. 1 è un diagramma a blocchi che illustra un sistema 100 per la generazione e l'archiviazione di metadati specifici dell'informatica forense. Il sistema 100 include il dispositivo informatico 102, che può comprendere un personal computer, un server, ecc., che comprende un'unità di elaborazione centrale („CPU") e una memoria che include dei software per l'esecuzione di varie attività (ad esempio, software del sistema operativo (OS), software applicativo, ecc.). I dati per il dispositivo informatico 102 possono essere memorizzati nella memoria del dispositivo stesso, nonché su altri dispositivi esterni come il server di backup 104, un compact disk, un'unità flash drive, un disco ottico e simili.

[0023] Nella presente esposizione, i dati di backup 106 provenienti dalla memoria del dispositivo 102 vengono trasmessi al server di backup 104 attraverso la rete 108. La rete 108 può essere Internet, una rete di telefonia mobile, una rete dati (ad esempio, una rete 4G o LTE), un Bluetooth o qualunque combinazione di questi elementi. Ad esempio, il server di backup 104 può far parte di un ambiente di cloud computing accessibile via Internet, oppure può far parte di una rete locale (LAN) con il dispositivo informatico 102. Le linee che collegano il server di backup 104 e il dispositivo informatico 102 alla rete

108 rappresentano i percorsi di comunicazione che possono includere qualunque combinazione di connessioni a spazio libero (ad es. per segnali wireless) e delle connessioni fisiche (ad es. cavi in fibra ottica).

[0024] Si noti che può esservi più di un server di backup 104, ma la FIG. 1 ne mostra uno solo per evitare di complicare ulteriormente il disegno. Ad esempio, il server di backup 104 può rappresentare una pluralità di server in un cluster cloud distribuito. Il server di backup 104 può comprendere qualunque numero di componenti fisici (come mostrato nella FIG. 5 ad esempio). Ad esempio, il server di backup 104 può comprendere una serie di componenti fisici come processori, dispositivi di archiviazione a blocchi fisici (ad esempio, unità di disco rigido (HDD), unità a stato solido (SSD), unità flash, dischi SMR, ecc.) o memorie (ad esempio, memoria ad accesso casuale (RAM)), componenti di interfaccia I/O, ecc.

[0025] I dati di backup 106 possono essere dati di qualunque tipo, inclusi dati utente, applicazioni, file di sistema, preferenze, documenti, supporti, ecc. Il dispositivo informatico 102 può inviare i dati di backup 106 per l'archiviazione sul server di backup 104 secondo un piano di backup indicante i dati specifici da includere nei dati di backup 106 e la frequenza con cui i dati devono essere sottoposti a backup. Ad esempio, il dispositivo informatico 102 può generare una copia di un file di dati esistente nella memoria del dispositivo 102 e trasmettere la copia in forma di dati di backup 106 al server di backup 104 ogni due ore. I dati di backup 106 possono essere selezionati da un utente del dispositivo informatico 102 e anche la frequenza del piano di backup può essere selezionata da un utente.

[0026] Come descritto sopra, sebbene il backup dei dati consenta di conservare le informazioni su un sistema (ad esempio il dispositivo informatico 102), la difesa da potenziali attività digitali sospette rende necessario salvare informazioni supplementari relative ai dati sul dispositivo informatico 106. Gli ingegneri forensi possono utilizzare queste informazioni supplementari per determinare l'origine di un'attività digitale sospetta e rilevare gli artefatti e le tracce residue dell'attività digitale sospetta sul dispositivo informatico 106. Poiché un'analisi forense può richiedere molto tempo, in quanto gli ingegneri devono estrarre manualmente i dati ed esaminare tutte le informazioni dato per dato, è necessario un metodo che riduca i tempi di triage delle prove, fornisca l'accesso al contenuto delle prove senza che i dati siano disarchiviati e autentichi i dati per garantire che non siano danneggiati.

[0027] Di conseguenza, la presente esposizione fornisce un metodo per la generazione e l'archiviazione di metadati specifici dell'informatica forense. Il modulo di digital forensics 110 comprende tre componenti, ossia: generatore di metadati specifici dell'informatica forense (FS) 112, analizzatore di attività 114 e dispositivo di notarizzazione 116. Il modulo di digital forensics 110 può risiedere sul dispositivo informatico 102 e può essere eseguito dall'elaboratore del dispositivo 102. Il modulo di digital forensics 110 può essere un software di backup diviso come thin client sul dispositivo 102 e come thick client sul server di backup 104 (o viceversa). In alcune realizzazioni, il modulo di digital forensics 110 può risiedere su un dispositivo esterno, come un server collegato al dispositivo informatico 102 attraverso la rete 108, o un percorso di comunicazione diretta (ad esempio un cavo USB).

[0028] Al fine di fornire ad un ingegnere forense le informazioni necessarie per condurre un'analisi forense in modo efficiente, il generatore di metadati FS 112 identifica i dati e i metadati pertinenti sul dispositivo informatico 102 che devono essere conservati separatamente in un archivio accessibile. In alcune realizzazioni, il generatore di metadati FS 112 può estrarre i metadati dei dati di backup 106 e archiviarli nel server di backup 104 come metadati FS 118. I metadati FS 118 possono includere vari attributi predeterminati dei dati di backup 106 che sono inclini a cambiare durante un'attività digitale sospetta. Tali attributi includono l'identificazione dei dati di backup 106, un percorso per i dati di backup 106, l'identificazione dei processi che utilizzano i dati di backup 106 e l'utilizzo della memoria associata ai dati di backup 106.

[0029] Il generatore di metadati FS 112 può raccogliere informazioni di sistema utilizzando varie funzioni e chiamate di sistema interne. Sebbene la raccolta di informazioni di sistema può essere eseguita su qualsiasi sistema operativo, per ragioni di sintesi, le funzioni di raccolta e chiamata dei metadati e discusse nella presente esposizione sono specifiche dei sistemi operativi Windows™. Va notato che il generatore di metadati FS 112 può impiegare funzioni e chiamate analoghe per estrarre metadati analoghi in qualunque altro sistema operativo in esecuzione sul dispositivo informatico 102.

[0030] Il generatore di metadati FS 112 può enumerare i processi utilizzando una qualsiasi delle seguenti funzioni: EnumProcesses, WTSEnumerateProcesses, CreateToolhelp32Snapshot, Process32First, Process32Next, NtQuerySystemInformation (SystemProcessAndThreadInformation).

[0031] Il generatore di metadati FS 112 può estrarre metadati quali nome, descrizione e ragione sociale di un file specificato da Path tramite API delle risorse: GetFileVersionInfoSize, GetFileVersionInfo e VerQueryValue. GetFileVersionInfoSize, GetFileVersionInfo e VerQueryValue.

[0032] Il generatore di metadati FS 112 può estrarre metadati come indirizzo di base, dimensione e loadcount di un file specificato tramite la funzione NtQuerySystemInformation (SystemProcessAndThreadInformation).

[0033] Il generatore di metadati FS 112 può estrarre metadati sull'uso della memoria di un processo specifico usando la funzione GetProcessMemoryInfo.

[0034] Il generatore di metadati FS 112 può estrarre metadati come la riga di comando e le informazioni della directory corrente utilizzando la funzione NtQueryInformationProcess, mentre la funzione ReadProcessMemory è usata per leggere dal Process Environment Block (PEB).

[0035] Il generatore di metadati FS 112 può estrarre metadati riguardanti un file DLL (Dynamic Link Library) come l'indirizzo di base della DLL, la dimensione della DLL e il loadcount della DLL, utilizzando la funzione EnumProcessModules. Inoltre, il generatore di metadati FS 112 può estrarre metadati relativi a un file DDL quali nome, descrizione e ragione sociale tramite Path attraverso le API delle risorse: GetFileVersionInfoSize, GetFileVersionInfo, VerQueryValue.

[0036] Il generatore di metadati FS 112 può estrarre metadati riguardanti un processo come le informazioni di temporizzazione utilizzando la funzione GetProcessTimes.

[0037] Il generatore di metadati FS 112 può estrarre metadati come un elenco di tutti gli handle aperti per ogni processo utilizzando la funzione NtQuerySystemInformation(SystemHandleInformation).

[0038] Il generatore di metadati FS 112 può estrarre metadati quali le impostazioni delle politiche di mitigazione di un processo (ad esempio, la politica di Address Space Layout Randomization (ASLR) o la Control Flow Guard (CFG)) utilizzando rispettivamente le funzioni GetProcessMitigationPolicy (ProcessASLRRPolicy) e GetProcessMitigationPolicy (ProcessControlFlowGuardGuardPolicy).

[0039] Il generatore di metadati FS 112 può estrarre metadati come una copia del descrittore di sicurezza per un oggetto specificato da un handle utilizzando la funzione GetSecurityInfo.

[0040] Il generatore di metadati FS 112 può estrarre metadati quali le informazioni su un token di accesso utilizzando la funzione GetTokenInformation(TokenUser). Un token di accesso è creato da un sistema, come il dispositivo informatico 102, quando un utente si connette. Ogni processo eseguito per conto dell'utente ha una copia del token di accesso. Il token di accesso identifica l'utente, i gruppi di utenti e i privilegi. Il generatore di metadati FS 112 può utilizzare la funzione PrivilegeCheck per determinare se un token di accesso possiede un determinato insieme di privilegi.

[0041] Il generatore di metadati FS 112 può estrarre metadati come la classe di priorità di un processo specificato insieme al valore di priorità di ogni thread del processo utilizzando rispettivamente le funzioni GetPriorityClass e GetThreadPriority.

[0042] Il generatore di metadati FS 112 può estrarre metadati dei servizi registrati in un processo come il nome del servizio, la descrizione, il percorso e lo stato. Allo stesso modo, il generatore FS 112 può estrarre metadati di thread come TID, ora di inizio, ora del kernel, ora dell'utente, stacktrace e stackwalk utilizzando le funzioni CreateToolhelp32Snapshot, Thread32First e Thread32Next.

[0043] Il generatore di metadati FS 112 può estrarre metadati come i nomi dei programmi lanciati al momento dell'avvio leggendo i valori delle seguenti chiavi di registro:

-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ Winlogon\Userinit

-HKEY _LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ Winlogon\Notify

-HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\ BootExecute

-HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

-HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

-HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices

-HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

-HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer\Run

-HKEY _CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer\Run

-HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ load

-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows

-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Winlogon\Notify

-HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell

-HKEY _LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ Winlogon\Shell

-HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\ ShellServiceObj ectDelayLoad

[0044] Il generatore di metadati FS 112 può estrarre metadati utilizzando uno strumento forense come il Volatility Framework™. Ad esempio, il generatore di metadati FS 112 può estrarre informazioni su processi nascosti usando il comando „psxview", può scansionare la memoria per verificare i driver caricati, scaricati e scollegati usando il comando „modscan" o „moddump", può trovare hook di funzione API/DLL usando il comando „apihooks", può trovare hook in una tabella descrittiva del servizio di sistema usando il comando „ssdt", può identificare gli hook dei pacchetti di richiesta I/O (IRP) usando il comando „driverirp" e può estrarre la tabella dei descrittori degli interrupt usando il comando „idt", può estrarre il buffer della cronologia dei comandi usando il comando „cmdscan", può estrarre le informazioni della console usando il comando „consoles", può identificare i servizi registrati in un sistema usando il comando „svcscan".

[0045] Il generatore di metadati FS 112 può estrarre metadati come le informazioni sui socket di rete (ad esempio, un elenco di endpoint TCP/UDP disponibili per un'applicazione) utilizzando le funzioni GetExtendedTcpTable e GetExtendedUdpTable.

[0046] Il generatore di metadati FS 112 può estrarre metadati come i record della tabella dei file master (MFT) che contengono informazioni dettagliate su un file su un volume di un file system NTFS, incluse le sue dimensioni, l'ora e la data, i permessi e il contenuto dei dati.

[0047] Il generatore di metadati FS 112 può estrarre metadati che dettagliano l'insieme degli identificatori di sessione di accesso esistenti (LUID), il numero di sessioni e le informazioni su una sessione di accesso specifica usando le funzioni LsaEnumerateLogonSessionSessionSessionData e LsaGetLogonSessionData.

[0048] Il generatore di metadati FS 112 può estrarre metadati come i log degli eventi di Windows usando la funzione ReadEventLog.

[0049] Il generatore di metadati FS 112 può estrarre metadati come ad esempio un elenco di file di contenuti del cestino usando le funzioni SHGetDesktopFolder e SHGetSpecialFolderLocation(CSIDL_BITBUCKET).

[0050] Il generatore di metadati FS 112 può estrarre metadati come l'IPv4 nella tabella di mappatura degli indirizzi fisici usando la funzione GetIpNetTable.

[0051] Il generatore di metadati FS 112 può estrarre metadati come le informazioni della cache DNS usando la funzione DnsQuery(DNS_QUERY_NO_WIRE_QUERY).

[0052] Il generatore di metadati FS 112 può generare uno screenshot usando le funzioni CreateCompatibleDC, CreateCompatibleBitmap, StretchBlt, BitBlt e GetDIBits.

[0053] I metadati supplementari che il generatore di metadati FS 112 può estrarre sono il nome del computer, il nome di dominio, il fuso orario, le variabili ambientali, le firme e i certificati. Per determinare metadati quali hash, profilo di entropia e stringhe, il generatore di metadati FS 112 può utilizzare speciali metodi di calcolo e di ricerca.

[0054] Il generatore di metadati FS 112 può generare metadati FS 118. I metadati FS 118 possono essere una struttura di dati (ad esempio un array) che aggrega qualunque combinazione dei metadati precedentemente descritti. Ad esempio, un primo campo della struttura di dati può indicare il nome del file di dati, un secondo campo della struttura di dati può indicare il percorso del file di dati, e così via.

[0055] Il generatore di metadati FS 112 può generare metadati FS 118 sulla base di regole predeterminate affinché venga selezionata una combinazione dei metadati sopra descritti e queste informazioni vengano raccolte periodicamente per il backup. Queste regole predeterminate possono essere memorizzate nella memoria del dispositivo informatico 102 o del server di backup 104. In un esempio, una regola può indicare, a seconda dello stato del dispositivo 102 (ad esempio, attività sospette rilevate o nessuna attività sospetta rilevata), che venga recuperato un certo insieme di metadati sopra descritti. In un esempio, una regola può indicare che, quando un'attività sospetta non viene rilevata, venga raccolto almeno uno degli elementi seguenti: identificatori di processi in esecuzione, informazioni sull'allocazione della memoria, identificatori di thread in esecuzione, informazioni sui privilegi di sicurezza, informazioni sul registro, identificatori di processi nascosti e percorsi di esecuzione automatica sul dispositivo informatico. Se viene rilevata un'attività sospetta, un'ulteriore serie di metadati può essere inclusa nell'elenco dei metadati specifici dell'informatica forense, quali identificatori di processi inattivi, identificativi di thread inattivi, ecc., in base alla regola predeterminata. Un'altra regola può indicare di ridurre il numero di tipi di metadati specifici dell'informatica forense da recuperare per il backup a seconda che il dispositivo informatico 102 sia inattivo (ad esempio, in modalità sleep). Un'altra regola ancora può indicare di ridurre il numero di tipi di metadati specifici dell'informatica forense da recuperare per il backup se la quantità di spazio libero nel server di backup 104 è inferiore allo spazio limite. E un'altra regola ancora può indicare di ridurre il numero di tipi di metadati specifici dell'informatica forense da recuperare per il backup se la frequenza del piano di backup è superiore alla frequenza di soglia (ad esempio, per garantire che il backup di dati non sia troppo impegnativo in termini di elaborazione o di memoria). In termini di riduzione,

la regola può specificare il numero esatto di tipi di metadati da recuperare. Ad esempio, se per impostazione predefinita vengono recuperati 20 tipi di metadati per il backup, la regola può indicare di ridurre il numero a 10 tipi di metadati.

[0056] L'analizzatore di attività 114 analizza gli attributi dei metadati FS 118 memorizzati sul dispositivo informatico 102 e può costituire la prima linea di difesa per rilevare attività digitali sospette. Ad esempio, i metadati FS 118 possono comprendere i processi elencati che vengono eseguiti sul dispositivo informatico 102 (ad esempio, recuperati dal generatore di metadati FS 112 attraverso la funzione EnumProcesses). L'analizzatore di attività 114 può quindi identificare processi estranei che non sono stati eseguiti da un utente autorizzato del dispositivo informatico 102. L'analizzatore di attività 114 può anche scansionare i metadati FS 118 per rilevare applicazioni e file di dati estranei che non sono stati installati da un utente autorizzato del dispositivo informatico 102. In risposta al rilevamento di un processo, di un'applicazione o di un file di dati estraneo, l'analizzatore di attività 114 può generare un evento di sicurezza indicante un'attività digitale sospetta sul dispositivo informatico 102. L'evento di sicurezza rappresenta un segnale che richiede l'esecuzione di un'indagine digitale. Come accennato in precedenza, eventuali ritardi nella segnalazione di attività digitali sospette possono essere onerosi. Prima che un ingegnere forense riesca ad esaminare il dispositivo informatico 102, questo potrebbe già essere stato danneggiato da un attacco informatico. Di conseguenza, in risposta all'individuazione di un'indicazione di attività digitale sospetta, viene immediatamente generato un evento di sicurezza. L'evento di sicurezza può essere, ad esempio, un'allerta per l'utente del dispositivo informatico 102 che sono state rilevate delle attività sospette.

[0057] In un esempio, l'analizzatore di attività 114 può contrassegnare i successivi backup dei dati utente (ad es. dati di backup 106) del piano di backup come potenzialmente interessati dall'attività digitale sospetta. In un esempio, l'analizzatore di attività 114 può ripristinare il dispositivo informatico 102 con un precedente backup dei dati di backup 106 generati prima dell'attività digitale sospetta. In particolare, l'analizzatore di attività 114 può trasmettere i dati di backup 106 e i metadati FS 118 al server di backup 104, entrambi con un indicatore segnalante che è stata rilevata un'attività digitale sospetta, e può recuperare, dal server di backup 104, una copia precedente dei dati di backup 106 che non include l'attività digitale sospetta da sostituire nel dispositivo informatico 102. In un esempio, il modulo di digital forensics aumenta anche la frequenza di generazione dei backup nel piano di backup dei metadati specifici dell'informatica forense.

[0058] E' descritto nel seguito come verificare l'autenticità dei dati analizzati in un'analisi forense. Generalmente, un ingegnere forense estrae i dati dal dispositivo informatico 102, ma è possibile che i dati estratti siano stati danneggiati dalla sospetta attività digitale. È anche possibile che il dispositivo informatico 102 abbia subito delle modifiche, come lo spegnimento o la formattazione, al punto che un ingegnere forense non è in grado di generare report accurati dei dati. Occorre pertanto verificare se i dati analizzati sono autentici e se non sono stati alterati in alcun modo.

[0059] Il dispositivo di notarizzazione 116 può generare un identificatore di notarizzazione del backup dei metadati specifici dell'informatica forense, in cui l'identificatore di notarizzazione è uno tra: un identificatore di transazione di blockchain, un valore di hash, una firma digitale o un codice di controllo. Il dispositivo di notarizzazione 116 può inoltre memorizzare un identificatore di notarizzazione con il backup dei metadati specifici dell'informatica forense. Ad esempio, il dispositivo di notarizzazione 116 può generare valori di hash dei metadati FS 118 nel dispositivo informatico 102 per abilitare questo processo di verifica. Quando i metadati FS 118 vengono trasmessi al server di backup 104, il dispositivo di notarizzazione 116 può utilizzare una funzione crittografica di hash per generare un valore hash di metadati FS 118 e successivamente aggiungere il valore hash al backup. In alcune realizzazioni, il dispositivo informatico 102 può trasmettere simultaneamente i dati di backup 106 e i metadati FS 118 al server di backup 104. Così, per tutti i dati di backup 106 sul server di backup 104, esistono metadati FS 118 con le relative informazioni sui metadati del dispositivo 102 (incluso un valore hash corrispondente). Memorizzando una prova di notarizzazione, come ad esempio un ID di transazione a blockchain, viene garantita l'autenticità dei metadati.

[0060] La FIG. 2 mostra un diagramma di flusso del metodo 200 per la generazione e l'archiviazione di metadati specifici dell'informatica forense. Al 202, il generatore di metadati FS 112 genera un backup dei dati utente memorizzati su un dispositivo informatico secondo un piano di backup. I dati di backup possono includere file di dati (ad es. foto, video, documenti, applicazioni, ecc.) e impostazioni associate all'utente. Il piano di backup può richiedere il backup periodico dei dati dell'utente identificato (ad esempio, una volta all'ora). Al 204, il generatore di metadati FS 112 identifica i metadati di sistema. In un esempio, supponiamo che i metadati di sistema siano informazioni sui thread inattivi. Questi metadati possono far parte di un elenco di metadati di sistema che possono essere recuperati dal generatore di metadati FS 112. Naturalmente, il recupero di tutti i metadati di sistema disponibili può richiedere molta memoria ed essere impegnativo per il elaboratore e per un ingegnere forense in termini di dati da rivedere. È pertanto necessario ridurre la quantità di metadati da sottoporre a backup poiché consente una migliore visibilità delle attività digitali sospette quando si considerano solo i metadati specifici dell'informatica forense.

[0061] Al 206, il generatore di metadati FS 112 determina se i metadati di sistema sono classificati come metadati specifici dell'informatica forense. Facendo riferimento all'esempio precedente, il generatore di metadati FS 112 può recuperare un elenco di regole predeterminate, di cui una può indicare che durante la normale attività (ad esempio, quando non viene rilevata alcuna attività digitale sospetta) le informazioni sui thread inattivi non devono essere memorizzate come parte dei metadati specifici dell'informatica forense. In risposta alla determinazione che i metadati di sistema non sono classificati come metadati specifici dell'informatica forense, il metodo 200 diventa 208, dove il generatore di metadati FS 112 determina se tutti i metadati di sistema sono stati presi in considerazione (ad esempio, se vi sono altri metadati di sistema non considerati nell'elenco dei metadati di sistema).

[0062] Al 208, il generatore di metadati FS 112 può determinare che vi sono altri metadati di sistema da considerare. Ne risulta che il metodo 200 ritorna al 204, dove vengono identificati diversi metadati di sistema. Per esempio, il generatore di metadati FS 112 può considerare metadati di sistema gli identificatori dei processi in esecuzione sul dispositivo informatico. Al 206, il generatore di metadati FS 112 può determinare che gli identificatori dei processi in esecuzione sono classificati come metadati specifici dell'informatica forense. In questo modo, al 210, il generatore di metadati FS 112 recupera i metadati di sistema (ad esempio, gli identificatori dei processi in esecuzione) per il backup come parte dei metadati specifici dell'informatica forense. Ad esempio, il generatore di metadati FS 112 può utilizzare le funzioni sopra descritte per enumerare i processi in esecuzione e raccogliere i rispettivi PID. Dal 210, il metodo 200 ritorna al 208 in modo che possano essere recuperati altri metadati specifici dell'informatica forense.

[0063] Se non devono essere considerati altri metadati di sistema al 208, il metodo 200 passa al 212, dove il generatore di metadati FS 112 genera un backup per i metadati specifici dell'informatica forense in conformità al piano di backup. Ad esempio, il generatore di metadati FS 112 può aggregare i metadati specifici dell'informatica forense recuperati e caricarli sul server di backup 104 tramite la rete 108.

[0064] Al 214, l'analizzatore di attività 114 può determinare se un'attività digitale sospetta è stata rilevata sulla base dei metadati specifici dell'informatica forense. Ulteriori dettagli sono dati con la descrizione della FIG. 3. In risposta al rilevamento dell'attività digitale sospetta, al 216, l'analizzatore di attività 114 genera un evento di sicurezza. Ad esempio, l'analizzatore di attività 114 può segnalare una richiesta di indagine digitale da parte di un ingegnere forense. Se non viene rilevata alcuna attività digitale sospetta, il metodo 200 ritorna al 202, dove ha inizio un altro ciclo di backup.

[0065] La FIG. 3 mostra un diagramma di flusso del metodo 300 per rilevare attività digitali sospette. Al 302, l'analizzatore di attività 114 può identificare un primo backup dei metadati specifici dell'informatica forense generato per la prima volta (ad esempio, nel ciclo precedente del piano di backup). Al 304, l'analizzatore di attività 114 identifica un secondo backup dei metadati specifici dell'informatica forense generati per la seconda volta dopo la prima volta (ad esempio, il backup corrente).

[0066] Al 306, l'analizzatore di attività 114 confronta i rispettivi backup per identificare un processo che esiste nel secondo backup e non nel primo backup. Se non viene trovato alcun processo, il metodo 300 ha fine. In risposta all'identificazione di un tale processo, l'analizzatore di attività 114 può determinare se il processo è fidato. Ad esempio, l'analizzatore di attività 114 può determinare se il processo è fidato confrontando il processo con una pluralità di processi fidati noti elencati in una struttura di dati. In risposta alla constatazione che non esiste alcuna corrispondenza tra il processo e un processo fidato noto nella pluralità di processi fidati noti, l'analizzatore di attività 114 può determinare che il processo non è fidato. Su queste basi, il metodo 300 passa a 312, dove l'analizzatore di attività 114 rileva un'indicazione di attività digitale sospetta sul dispositivo informatico.

[0067] Se il processo è effettivamente fidato (ad. es. si trova nell'elenco dei processi fidati), il metodo 300 passa invece a 310, dove l'analizzatore di attività 114 non rileva alcuna attività digitale sospetta sul dispositivo informatico.

[0068] La FIG. 4 mostra un diagramma di flusso del metodo 400 per aggiornare il piano di backup basato sulla rilevazione di attività digitali sospette. Il metodo 400 può essere eseguito dal modulo di digital forensics 110 dopo che l'analizzatore di attività 114 ha generato un evento di sicurezza al 216 del metodo 200. Al 402, il generatore di metadati FS 112 può aumentare la frequenza del piano di backup. Supponiamo che la frequenza del piano di backup sia una volta al minuto. È possibile che un vero e proprio attacco informatico non si sia ancora verificato e che qualsiasi attività digitale sospetta rilevata sia parte di un potenziale attacco informatico. Al fine di migliorare la granularità delle informazioni per un ingegnere forense che esegue un'indagine digitale, la frequenza dei backup e la quantità di dettagli mirati sulle attività sospette dovrebbe aumentare. Di conseguenza, al 402, il generatore di metadati FS 112 può aumentare la frequenza del piano di backup - in particolare per i metadati specifici dell'informatica forense - a ogni 10 secondi (invece che ogni minuto).

[0069] Al 404, l'analizzatore di attività 114 può identificare una caratteristica dell'attività digitale sospetta. Ad esempio, l'attività digitale sospetta può essere l'esecuzione di un processo non fidato. La caratteristica dell'attività digitale sospetta può quindi essere il PID del processo. Al 406, il generatore di metadati FS 112 può identificare metadati di sistema per dettagli avanzati sull'attività digitale sospetta in base alla caratteristica. Ad esempio, il generatore di metadati FS 112 può inizialmente recuperare esclusivamente i PID dei processi in esecuzione. In risposta all'identificazione della caratteristica, il generatore di metadati FS 112 può iniziare a monitorare ulteriori dettagli sul processo non fidato come l'uso della memoria, i privilegi di sicurezza e le informazioni sul thread.

[0070] Al 408, il generatore di metadati FS 112 recupera i metadati di sistema identificati come parte di metadati specifici dell'informatica forense. Il metodo 400 passa quindi al 202 del metodo 200. Di conseguenza, durante la seconda iterazione del metodo 200 (ad esempio, dopo che è stata rilevata un'attività sospetta), i successivi backup di metadati specifici dell'informatica forense avverranno più frequentemente e con ulteriori dettagli sull'attività digitale sospetta (come parte di avanzati metadati specifici dell'informatica forense).

[0071] La FIG. 5 è un diagramma a blocchi che mostra un sistema informatico 20 su cui possono essere implementati sistemi e metodi di archiviazione e generazione di metadati specifici dell'informatica forense. Il sistema informatico 20 può rappresentare il dispositivo informatico 102 e/o il server di backup 104 e può essere sotto forma di più dispositivi informatici, o sotto forma di un singolo dispositivo informatico, ad esempio un computer da tavolo, un notebook, un laptop, un dispositivo

informatico mobile, uno smartphone, un tablet, un server, un computer centrale, un dispositivo integrato e altre forme di dispositivi informatici.

[0072] Come mostrato, il sistema informatico 20 comprende 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 può comprendere una memoria del bus o un controller di memoria del bus, un bus periferico e un bus locale in grado di interagire con qualsiasi altra architettura di bus. Esempi di bus possono includere PCI, ISA, PCI-Express, HyperTransport™, InfiniBand™, Serial ATA, I2C e altre interconnessioni adeguate. L'unità di elaborazione centrale 21 (detta anche elaboratore) può comprendere un singolo o una serie di processori con uno o più core. Il elaboratore 21 può eseguire uno o più codici informatici eseguibili che implementano le tecniche della presente esposizione. Ad esempio, uno qualunque dei metodi 200-400 eseguiti dal modulo di digital forensics 110 (ad esempio, attraverso i suoi componenti, come il generatore di metadati FS 112) può essere eseguito dall'elaboratore 21. La memoria di sistema 22 può essere qualunque memoria per la memorizzazione dei dati qui utilizzati e/o programmi informatici eseguibili dal elaboratore 21. La memoria di sistema 22 può includere una memoria volatile come una memoria ad accesso casuale (RAM) 25 e una memoria non volatile come una memoria di sola lettura (ROM) 24, una memoria flash, ecc. o una combinazione di queste. Il sistema di base di input/output (BIOS) 26 può memorizzare 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'uso della ROM 24.

[0073] Il sistema informatico 20 può comprendere 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 di questi. 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 informatici sono moduli indipendenti dalla potenza per la memorizzazione di istruzioni, 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 possono utilizzare una varietà di supporti di archiviazione informatici. Esempi di supporti di archiviazione informatici includono la memoria a bordo macchina come cache, SRAM, DRAM, RAM a zero condensatori, RAM a doppio transistor, eDRAM, EDO RAM, DDR RAM, EEPROM, NRAM, RRAM, SONOS, PRAM; memoria flash o altre tecnologie di memoria come nelle unità a stato solido (SSD) o unità flash; cassette magnetiche, nastri magnetici e memorizzazione su dischi magnetici come, ad esempio, in unità disco rigido o floppy disk; memorizzazione ottica come, ad esempio, in compact disk (CD-ROM) o dischi digitali versatili (DVD); e qualsiasi altro supporto che può essere utilizzato per memorizzare i dati desiderati e che possa essere accessibile dal sistema informatico 20.

[0074] La memoria di sistema 22, i dispositivi di archiviazione rimovibili 27 e i dispositivi di archiviazione non rimovibili 28 del sistema informatico 20 possono essere utilizzati per memorizzare un sistema operativo 35, applicazioni aggiuntive di programmi 37, altri moduli di programma 38 e dati di programma 39. Il sistema informatico 20 può includere un'interfaccia periferica 46 per la comunicazione dei dati provenienti dai dispositivi di input 40, come tastiera, mouse, stilo, controller di gioco, dispositivo a comandi vocali, dispositivo a comandi tattili o altri dispositivi periferici, come stampante o scanner tramite una o più porte I/O, come una porta seriale, una porta parallela, un bus seriale universale (USB) o un'altra interfaccia periferica. Un dispositivo di visualizzazione 47, come uno o più monitor, proiettori o display integrato, possono anche essere collegati al bus di sistema 23 attraverso un'interfaccia di uscita 48, come un adattatore video. Oltre ai dispositivi di visualizzazione 47, il sistema informatico 20 può essere dotato di altri dispositivi periferici di uscita (non mostrati), come altoparlanti e altri dispositivi audiovisivi.

[0075] Il sistema informatico 20 può funzionare in un ambiente di rete utilizzando una connessione di rete a uno o più computer remoti 49. Il computer remoto (o i computer) 49 può essere costituito da postazioni di lavoro locali o server che comprendono la maggior parte o tutti gli elementi menzionati sopra nella descrizione della natura di un sistema informatico 20. Nella rete informatica possono essere presenti anche altri dispositivi, quali, ma non solo, router, stazioni di rete, dispositivi peer o altri nodi di rete. Il sistema informatico 20 può comprendere una o più interfacce di rete 51 o adattatori di rete per comunicare con i computer remoti 49 attraverso una o più reti, quali una rete informatica locale (LAN) 50, una rete informatica ad ampio raggio (WAN), una intranet e Internet. Esempi di interfaccia di rete 51 possono includere un'interfaccia Ethernet, un'interfaccia Frame Relay, un'interfaccia SONET e interfacce wireless.

[0076] La presente esposizione descrive un sistema, un metodo e/o un prodotto di un programma informatico. Il prodotto del programma informatico può includere un supporto di archiviazione informatico (o supporti) con istruzioni per programmi informatici per far sì che un elaboratore esegua aspetti della presente esposizione.

[0077] Il supporto di archiviazione informatico può essere un dispositivo tangibile in grado di conservare e memorizzare il codice del programma sotto forma di istruzioni o strutture di dati accessibili da un elaboratore di un dispositivo informatico, come il sistema informatico 20. Il supporto di archiviazione informatico può essere un dispositivo di archiviazione elettronica, un dispositivo di archiviazione magnetica, un dispositivo di archiviazione ottica, un dispositivo di archiviazione elettromagnetica, un dispositivo di archiviazione a semiconduttori o qualunque combinazione appropriata di questi. A titolo di esempio, tale supporto di archiviazione informatico può comprendere una memoria ad accesso casuale (RAM), una memoria a sola lettura (ROM), una EEPROM, una memoria a sola lettura di un compact disc portatile (CD-ROM), un disco digitale versatile (DVD), una memoria flash, un disco rigido, un dischetto portatile, un memory stick, un floppy disk, o anche un dispositivo codificato meccanicamente come schede perforate o strutture in rilievo in un solco con istruzioni registrate.

Come utilizzato nel presente, un supporto di archiviazione informatico non è da intendersi come segnali transitori di per sé, come onde radio o altre onde elettromagnetiche che si propagano liberamente, onde elettromagnetiche che si propagano attraverso una guida d'onda o un mezzo di trasmissione, o segnali elettrici trasmessi attraverso un filo.

[0078] Le istruzioni di programmi informatici descritte nel presente documento possono essere scaricate sui rispettivi dispositivi informatici da un supporto di archiviazione informatico o su un computer esterno o un dispositivo di archiviazione esterno attraverso una rete, ad esempio Internet, una rete locale, una rete ad ampio raggio e/o una rete wireless. La rete può comprendere cavi di trasmissione in rame, fibre ottiche di trasmissione, trasmissione senza fili, router, firewall, switch, computer gateway e/o server di bordo. Un'interfaccia di rete di ogni dispositivo informatico riceve dalla rete istruzioni di programmi informatici e inoltra le istruzioni di programmi informatici per l'archiviazione in un supporto di archiviazione informatico all'interno del rispettivo dispositivo informatico.

[0079] Le istruzioni di programmi informatici per l'esecuzione delle operazioni della presente esposizione possono essere istruzioni di assemblaggio, insiemi di istruzioni (ISA), istruzioni per macchine, istruzioni dipendenti dalla macchina, microcodici, istruzioni firmware, dati di impostazione dello stato, oppure codici sorgente o codici oggetto scritti in qualunque combinazione di uno o più linguaggi di programmazione, compreso un linguaggio di programmazione orientato agli oggetti e linguaggi di programmazione procedurali convenzionali. Le istruzioni di programmi informatici possono essere eseguite interamente sul computer dell'utente, in parte sul computer dell'utente, come pacchetto software indipendente, in parte sul computer dell'utente e in parte su un computer remoto o interamente sul computer o server remoto. In quest'ultimo caso, il computer remoto può essere collegato al computer dell'utente attraverso qualunque tipo di rete, compresa una rete LAN o WAN, oppure la connessione può essere effettuata a un computer esterno (ad esempio, attraverso Internet). In alcune realizzazioni, i circuiti elettronici che comprendono, ad esempio, circuiti a logica programmabile, gate array programmabili sul campo (FPGA), o array a logica programmabile (PLA) possono eseguire le istruzioni di programmi informatici utilizzando le informazioni di stato delle istruzioni di programmi informatici per personalizzare i circuiti elettronici.

[0080] I sistemi e i metodi descritti nella presente esposizione possono essere trattati in termini di moduli. Il termine „modulo" qui utilizzato si riferisce a un dispositivo reale, componente o disposizione di componenti, realizzato utilizzando hardware, come ad esempio tramite un circuito integrato specifico di un'applicazione (ASIC) o FPGA, o come una combinazione di hardware e software, come ad esempio tramite un sistema a microprocessore e un insieme di istruzioni per implementare le funzionalità del modulo, che (mentre viene eseguito) trasforma il sistema a microprocessore in un dispositivo speciale. Un modulo può anche essere implementato come una combinazione dei due, con alcune funzioni facilitate solo dall'hardware e altre funzioni facilitate da una combinazione di hardware e software. In alcune implementazioni, almeno una parte e, in alcuni casi tutti, i moduli possono essere eseguiti sull'elaboratore di un sistema informatico. Di conseguenza, ogni modulo può essere realizzato in una varietà di configurazioni adatte e non deve essere limitato ad una particolare implementazione qui esemplificata.

[0081] Per motivi di chiarezza, non tutte le caratteristiche di routine sono qui riportate. Sarebbe auspicabile che nello sviluppo di qualsiasi implementazione effettiva della presente esposizione vengano prese numerose decisioni specifiche dell'implementazione al fine di raggiungere gli obiettivi specifici dello sviluppatore e questi obiettivi specifici variano a seconda delle diverse implementazioni e dei diversi sviluppatori. Resta inteso che un tale sforzo di sviluppo potrebbe essere complesso e richiederebbe molto tempo, ma sarebbe comunque un'impresa facile per coloro che hanno un'ordinaria competenza nell'arte che si avvantaggiano di questa esposizione.

[0082] Inoltre, è da intendersi che la fraseologia o la terminologia qui utilizzata ha lo scopo di descrizione e non di restrizione, cosicché la terminologia o la fraseologia della presente specifica deve essere interpretata da chi è competente nell'arte alla luce degli insegnamenti e degli orientamenti qui presentati, in combinazione con le conoscenze di chi è competente nell'arte o nelle arti pertinenti. Inoltre, a nessun termine della specifica o rivendicazione deve essere attribuito un significato non comune o speciale, a meno che non sia esplicitamente indicato come tale.

Rivendicazioni

1. Metodo per l'archiviazione di metadati specifici dell'informatica forense, in cui il metodo comprende:
   generare un backup dei dati utente archiviati su un dispositivo informatico conformemente a un piano di backup;
   identificare, da una pluralità di metadati di sistema del dispositivo informatico, i metadati specifici dell'informatica forense del dispositivo informatico basati su regole predeterminate, in cui i metadati specifici dell'informatica forense sono utilizzati per rilevare attività digitali sospette;
   generare un backup dei metadati specifici dell'informatica forense in conformità al piano di backup, in cui il backup dei metadati specifici dell'informatica forense è archiviato separatamente dal backup dei dati dell'utente;
   analizzare i metadati specifici dell'informatica forense per rilevare un'indicazione di un'attività digitale sospetta sul dispositivo informatico; e
   in risposta all'individuazione dell'attività digitale sospetta sulla base dell'analisi. generare un evento di sicurezza indicante che l'attività digitale sospetta si è verificata,
   in cui l'evento di sicurezza è un segnale di allerta.
2. Metodo secondo la rivendicazione 1, in cui generare l'evento di sicurezza comprende anche la contrassegnazione dei successivi backup dei dati utente del piano di backup come potenzialmente interessati dall'attività digitale sospetta.

3. Metodo secondo una qualunque delle rivendicazioni da 1 a 2, in cui generare l'evento di sicurezza comprende anche la richiesta di esecuzione di un'indagine digitale.

4. Metodo secondo una qualunque delle rivendicazioni da 1 a 3, in cui la generazione dell'evento di sicurezza comprende anche il ripristino del dispositivo informatico con un precedente backup dei dati utente generati prima dell'attività digitale sospetta.

5. Metodo secondo una qualunque delle rivendicazioni da 1 a 4, in cui la generazione dell'evento di sicurezza comprende anche l'aumento della frequenza di generazione dei backup nel piano di backup dei metadati specifici dell'informatica forense.

6. Metodo secondo una qualunque delle rivendicazioni da 1 a 5, in cui i metadati specifici dell'informatica forense comprendono almeno uno tra: un identificatore di un processo in esecuzione,
informazioni sull'allocazione della memoria,
un identificatore di un thread in esecuzione,
informazioni sui privilegi di sicurezza,
informazioni di registro,
un identificatore di un processo nascosto, e
un percorso di esecuzione automatica sul dispositivo informatico.

7. Metodo secondo una qualunque delle rivendicazioni da 1 a 6, comprendente inoltre:
generare un identificatore di notarizzazione del backup dei metadati specifici dell'informatica forense, in cui l'identificatore di notarizzazione è uno tra: un identificatore di transazione di blockchain, un valore di hash, una firma digitale o un codice di controllo; e
memorizzare l'identificatore di notarizzazione con il backup dei metadati specifici dell'informatica forense.

8. Metodo secondo una qualunque delle rivendicazioni da 1 a 7, in cui l'analisi dei metadati specifici dell'informatica forense per l'indicazione di attività digitali sospette comprende:
identificare un primo backup dei metadati specifici dell'informatica forense generato la prima volta e un secondo backup dei metadati specifici dell'informatica forense generato una seconda volta dopo la prima volta;
rilevare, a partire dai metadati specifici dell'informatica forense, un processo nel secondo backup non presente nel primo backup; e
determinare se il processo è fidato; e
in risposta alla constatazione che il processo non è fidato, rilevare l'indicazione dell'attività digitale sospetta sul dispositivo informatico.

9. Metodo secondo la rivendicazione 8, in cui determinare se il processo è fidato comprende:
confrontare il processo con una pluralità di processi fidati noti elencati in una struttura di dati; e
determinare che non esiste alcuna corrispondenza tra il processo e un processo fidato noto nella pluralità di processi fidati noti.

10. Metodo secondo una qualunque delle rivendicazioni da 1 a 9, in cui generare l'evento di sicurezza comprende anche:
identificare le caratteristiche dell'attività digitale sospetta, dette caratteristiche includendo un identificativo di processo PID dell'attività digitale sospetta;
identificare metadati avanzati specifici dell'informatica forense sulla base delle caratteristiche, in cui i metadati avanzati specifici dell'informatica forense comprendono dettagli specifici delle caratteristiche dell'attività digitale sospetta, compreso l'uso della memoria o un privilegio di sicurezza; e
generare backup successivi dei metadati avanzati specifici dell'informatica forense.

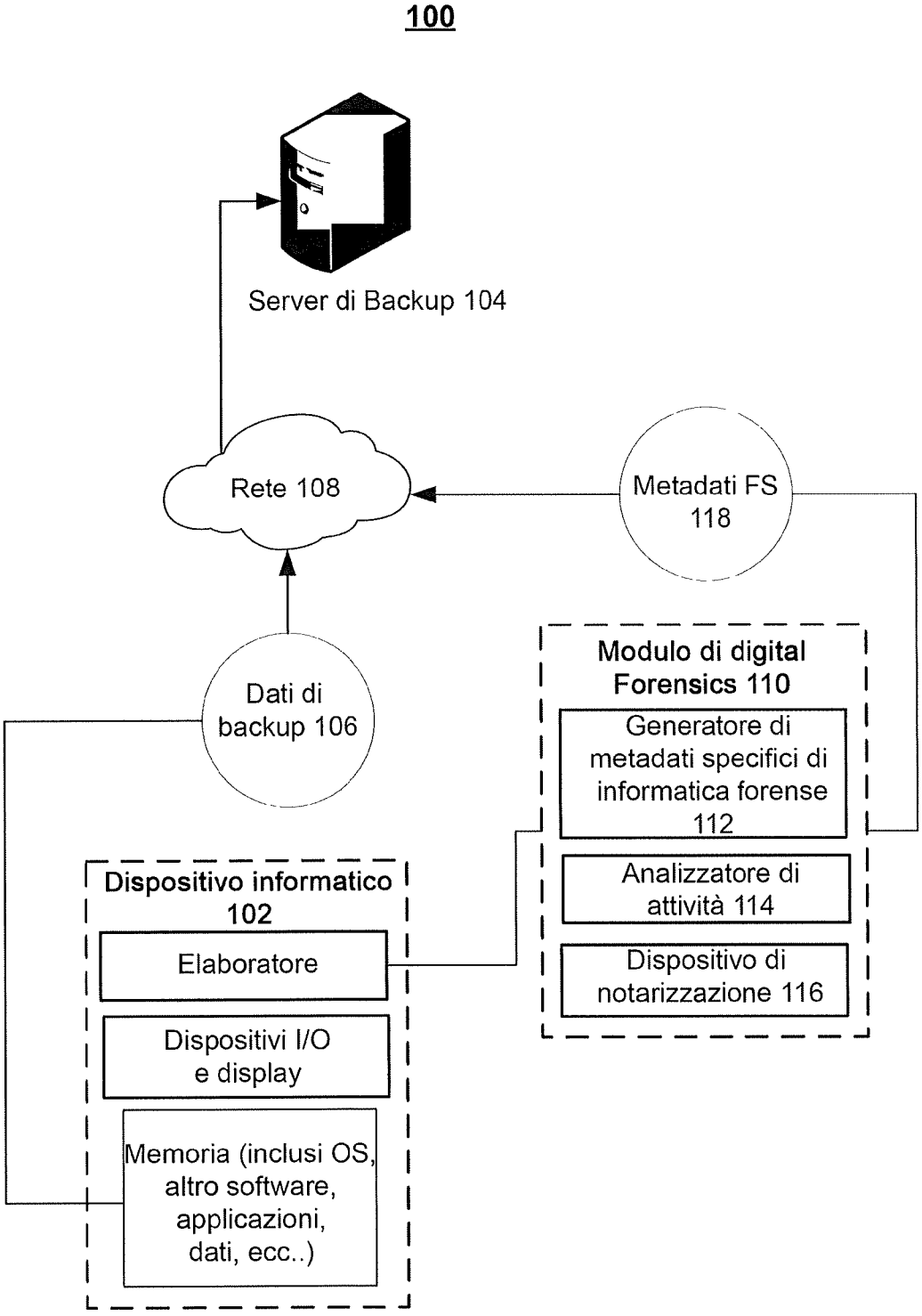

100
Server di Backup 104
Rete 108
Metadati FS 118
Modulo di digital Forensics 110
Generatore di metadati specifici di informatica forense 112
Analizzatore di attività 114
Dispositivo di notarizzazione 116
Dati di backup 106
Dispositivo informatico 102
Elaboratore
Dispositivi I/O e display
Memoria (inclusi OS, altro software, applicazioni, dati, ecc..)

FIG. 1

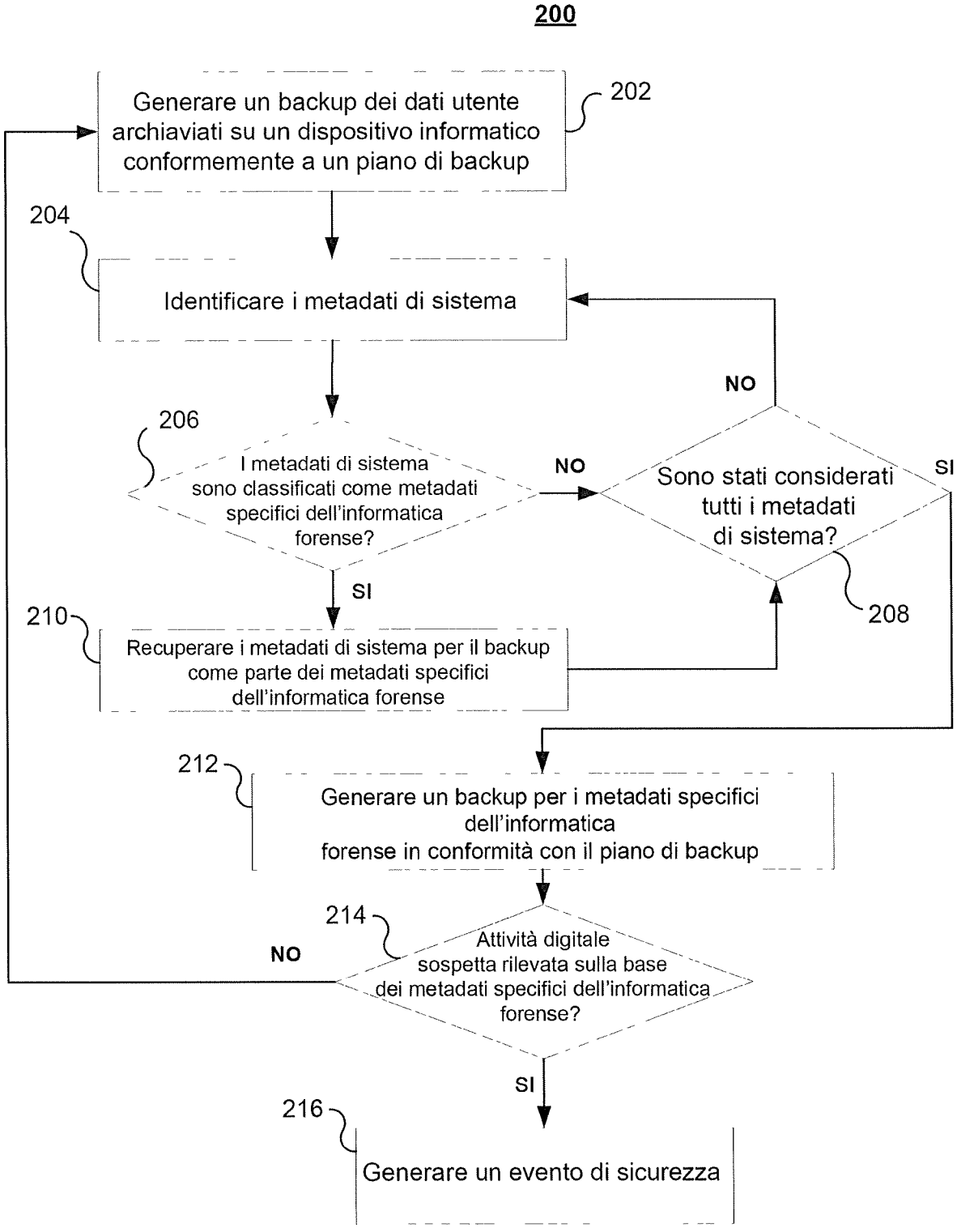

200
Generare un backup dei dati utente archiviati su un dispositivo informatico conformemente a un piano di backup
202
204
Identificare i metadati di sistema
206
I metadati di sistema sono classificati come metadati specifici dell'informatica forense?
NO
Sono stati considerati tutti i metadati di sistema?
NO
SI
208
SI
210
Recuperare i metadati di sistema per il backup come parte dei metadati specifici dell'informatica forense
212
Generare un backup per i metadati specifici dell'informatica forense in conformità con il piano di backup
214
Attività digitale sospetta rilevata sulla base dei metadati specifici dell'informatica forense?
NO
SI
216
Generare un evento di sicurezza

FIG. 2

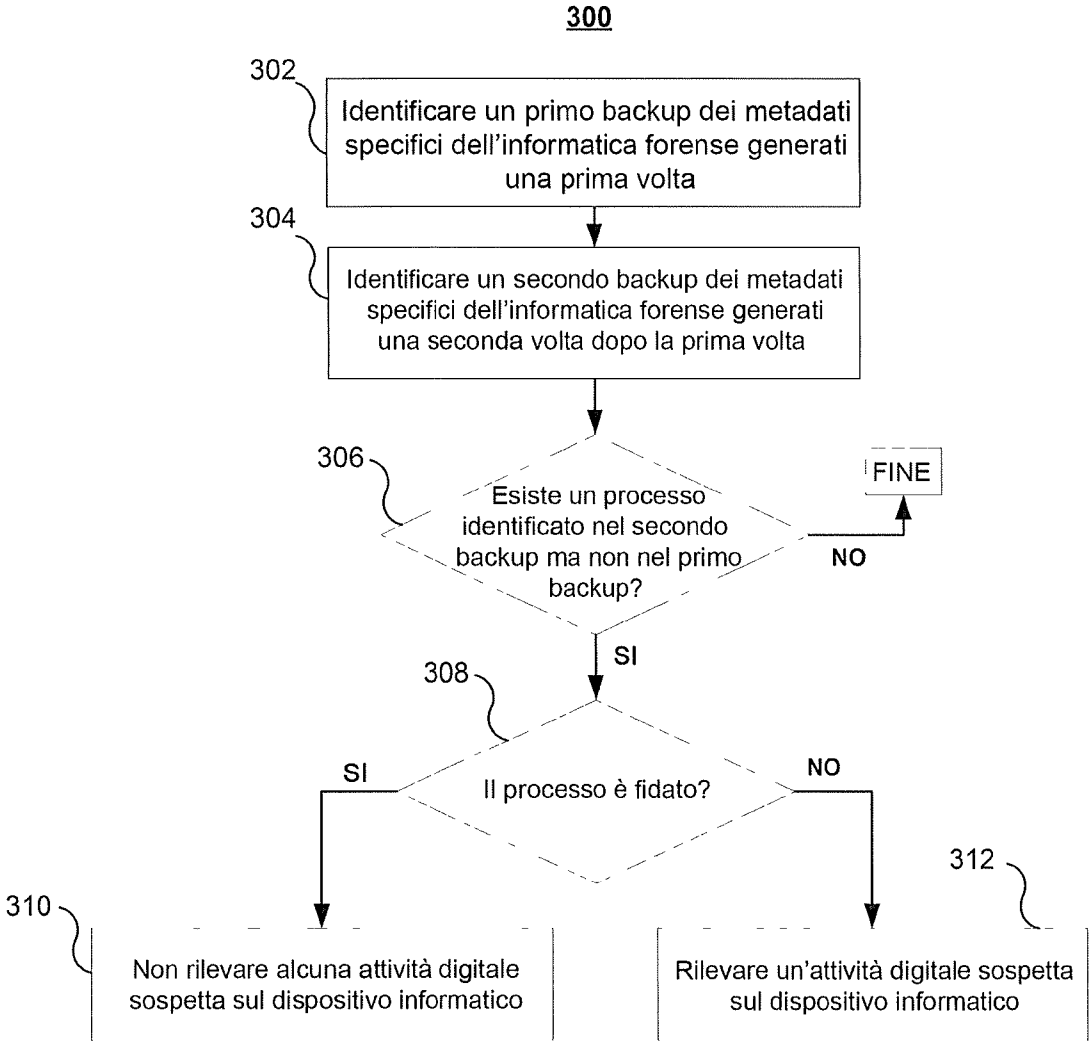

300
302
Identificare un primo backup dei metadati specifici dell'informatica forense generati una prima volta
304
Identificare un secondo backup dei metadati specifici dell'informatica forense generati una seconda volta dopo la prima volta
306
Esiste un processo identificato nel secondo backup ma non nel primo backup?
NO
FINE
SI
308
Il processo è fidato?
SI
NO
310
Non rilevare alcuna attività digitale sospetta sul dispositivo informatico
312
Rilevare un'attività digitale sospetta sul dispositivo informatico

FIG. 3

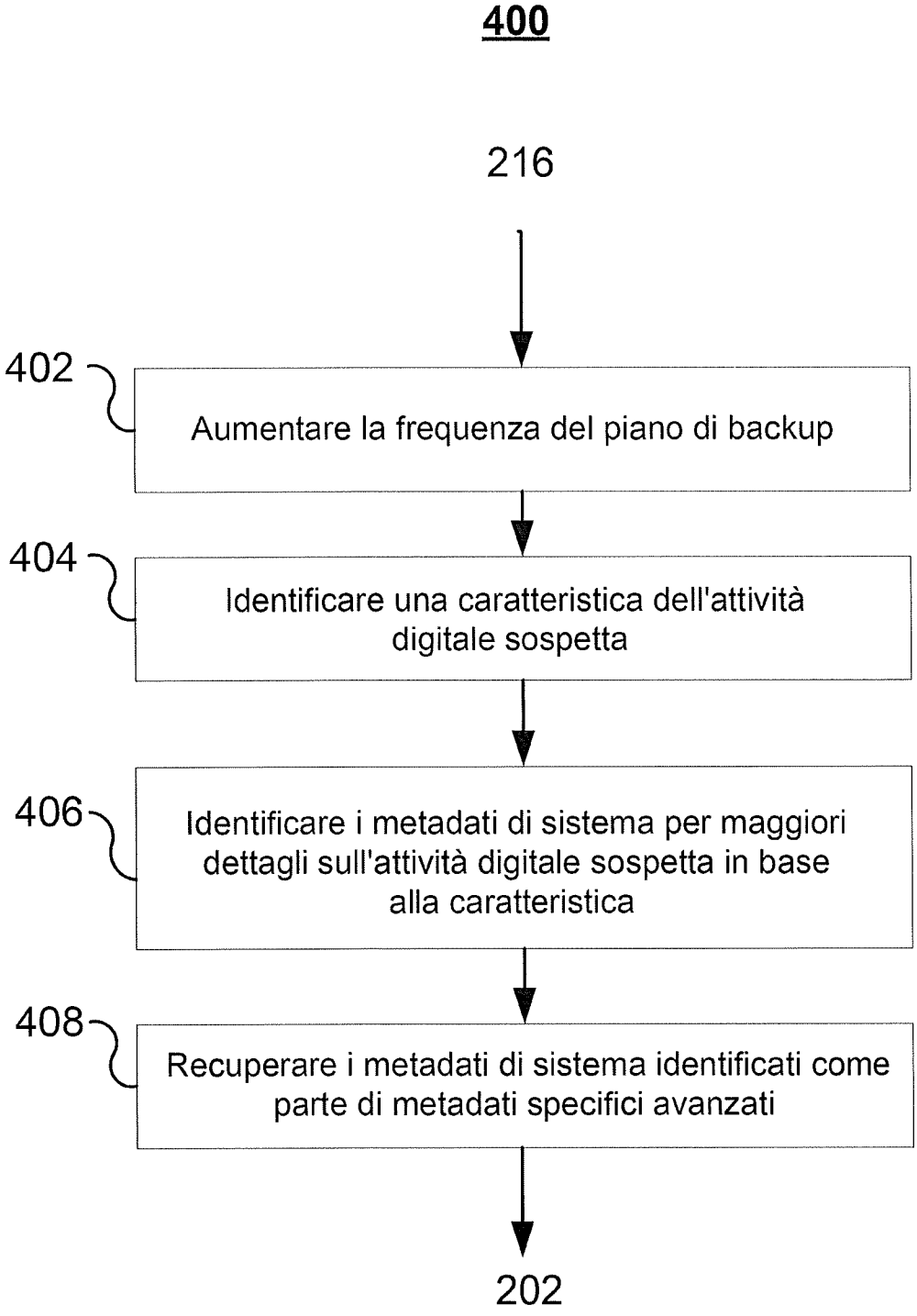

400
216
402
Aumentare la frequenza del piano di backup
404
Identificare una caratteristica dell'attività digitale sospetta
406
Identificare i metadati di sistema per maggiori dettagli sull'attività digitale sospetta in base alla caratteristica
408
Recuperare i metadati di sistema identificati come parte di metadati specifici avanzati
202

FIG. 4

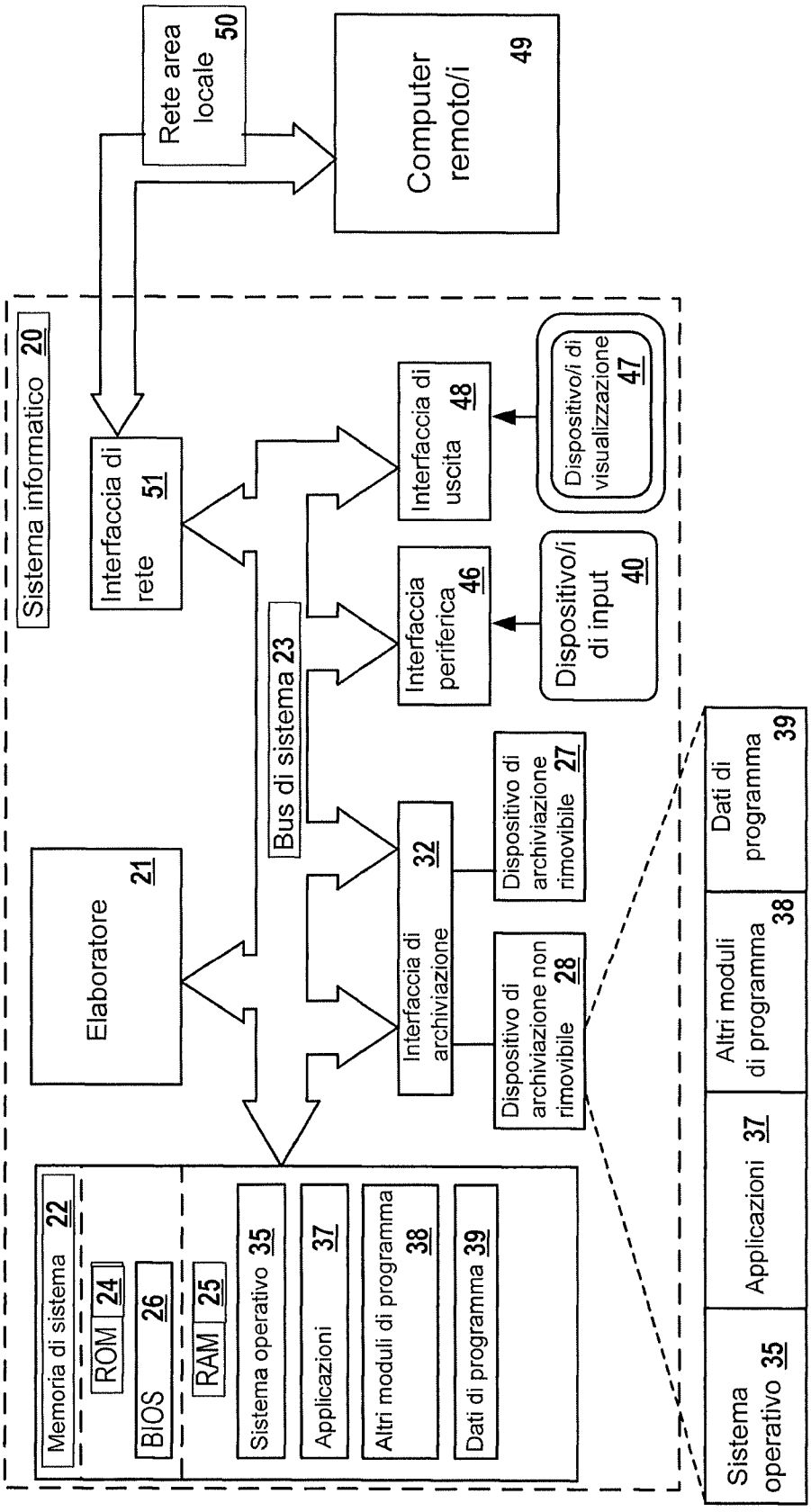

Rete area locale 50
Computer remoto/i 49
Sistema informatico 20
Interfaccia di rete 51
Interfaccia di uscita 48
Dispositivo/i di visualizzazione 47
Interfaccia periferica 46
Dispositivo/i di input 40
Bus di sistema 23
Elaboratore 21
Interfaccia di archiviazione 32
Dispositivo di archiviazione rimovibile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

FIG. 5