



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0065819
(43) 공개일자 2012년06월21일

(51) 국제특허분류(Int. Cl.)

G06F 21/24 (2006.01) G06F 17/40 (2006.01)

G06F 17/30 (2006.01)

(21) 출원번호 10-2010-0127132

(22) 출원일자 2010년12월13일

심사청구일자 없음

(71) 출원인

한국전자통신연구원

대전광역시 유성구 가정로 218 (가정동)

고려대학교 산학협력단

서울 성북구 안암동5가 1

(72) 발명자

최우용

대전광역시 유성구 엑스포로 448, 304동 1204호
(전민동, 엑스포아파트)

은성경

대전광역시 유성구 엑스포로 448, 404동 1106호
(전민동, 엑스포아파트)

(뒷면에 계속)

(74) 대리인

김원준, 제일특허법인

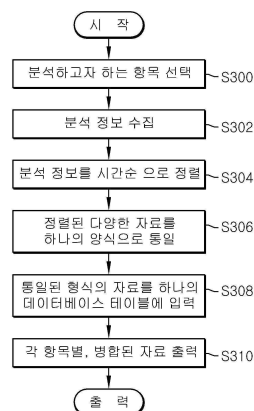
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 사용자 행위 분석을 위한 디지털 포렌식 장치 및 그 방법

(57) 요약

본 발명은 컴퓨터 등 다양한 컴퓨팅 시스템에서 사용자가 특정 시간에 무슨 행위를 하였는가를 알 수 있도록 사용자 행위 분석을 파악 수 있는 자료들을 수집 및 가공하여 시간 순서에 따라 조사자가 원하는 의미 있는 자료들을 수집하고, 수집된 자료들을 자동적으로 분석하여 시간 순서로 표시시켜줌으로써, 디지털 포렌식 조사를 빠르고 효율적으로 할 수 있도록 한다. 또한, 본 발명에서와 같이 특정 시스템에서 사용자의 행위에 대해 시간 순서대로 표시하여줌으로써 조사자가 특정 시간대에 일어난 일들을 상세하면서도 쉽게 인지할 수 있으며, 여러 도구를 사용하여 수집을 하지 않고 하나의 도구로 분석을 수행할 수 있기 때문에 조사시간을 상당히 줄일 수 있다.

대표도 - 도3



(72) 발명자

홍도원

대전광역시 유성구 엑스포로 448, 212동 1704호
(전민동, 엑스포아파트)

이상진

서울특별시 노원구 중계동 363 대림벽산아파트
103동 1102호

방제완

서울특별시 성북구 인촌로16길 4-25, 102호 (안암
동3가)

박정흠

경기도 부천시 소사구 심곡본1동 아름다운나날아
파트 101동 904호

손남훈

서울특별시 서대문구 북아현로11나길 21 (북아현
동)

이 발명을 지원한 국가연구개발사업

과제고유번호 10035157

부처명 지식경제부/방송통신위원회

연구사업명 정보통신산업원천기술개발사업

연구과제명 실시간 분석을 위한 디지털 포렌식 기술 개발

주관기관 한국전자통신연구원

연구기간 2010.03.01 ~ 2011.02.28

특허청구의 범위

청구항 1

사용자 행위 분석이 필요한 대상 장치로부터 사용자 행위와 관련된 분석 정보를 수집하는 수집부와,
상기 수집부로부터 수집되는 상기 분석 정보를 분석하여 각 분석 정보별 사용자의 행위 정보를 파악하고, 상기 행위 정보를 시간 순서대로 정렬하여 표시시키는 분석부를 포함하는 사용자 행위 분석을 위한 디지털 포렌식 장치.

청구항 2

제 1 항에 있어서,

상기 수집부는,

상기 분석 정보 중 조사자에 의해 선택되는 분석 정보 항목을 입력받은 후, 상기 입력받는 항목에 대한 분석 정보를 상기 장치로부터 수집하는 사용자 행위 분석을 위한 디지털 포렌식 장치.

청구항 3

제 1 항에 있어서,

상기 분석부는,

상기 행위 정보를 하나의 양식으로 통일하고 데이터베이스 테이블에 입력하는 사용자 행위 분석을 위한 디지털 포렌식 장치.

청구항 4

제 1 항에 있어서,

상기 분석 정보는,

상기 장치의 파일 시스템 정보, 레지스트리 정보, 이벤트 로그 정보, 프리페치 정보, 웹브라우저 정보, 로그 파일 정보 중 적어도 하나 이상을 포함하는 사용자 행위 분석을 위한 디지털 포렌식 장치.

청구항 5

제 4 항에 있어서,

상기 분석부는,

상기 분석 정보 중 레지스트리 정보를 수신하는 경우, 상기 레지스트리 정보의 분석을 통해 상기 장치에 USB 드라이브 장착이나 응용 프로그램 설치 여부를 판단하여 상기 사용자의 행위 정보로 생성하는 사용자 행위 분석을 위한 디지털 포렌식 장치.

청구항 6

제 5 항에 있어서,

상기 분석부는,

상기 레지스트리 정보 중 MRU(most recently used) 킷값을 이용하여 상기 장치에서 문서 사용 여부를 판단하고, 이를 사용자의 행위 정보로 생성하는 사용자 행위 분석을 위한 디지털 포렌식 장치.

청구항 7

제 1 항에 있어서,

상기 행위 정보는,

응용 프로그램 설치, USB 저장장치 장착, 문서 사용, 프로그램 실행, 웹사이트 방문과 검색, 특정 시각의 파일 수정과 생성 중 적어도 하나 이상을 포함하는 사용자 행위 분석을 위한 디지털 포렌식 장치.

청구항 8

사용자 행위 분석이 필요한 대상 장치로부터 사용자 행위와 관련된 분석 정보를 수집하는 단계와,

상기 수집한 분석 정보를 분석하여 각 분석 정보별 사용자의 행위 정보를 파악하는 단계와,

상기 행위 정보를 시간 순서대로 정렬하여 표시시키는 단계

를 포함하는 사용자 행위 분석을 위한 디지털 포렌식 조사 방법.

청구항 9

제 8 항에 있어서,

상기 수집하는 단계는,

사용자 행위 분석이 필요한 대상 장치에 대해 수집할 분석 정보 항목을 입력받는 단계와,

상기 입력받은 항목에 대한 분석 정보를 상기 장치로부터 수집하는 단계

를 포함하는 사용자 행위 분석을 위한 디지털 포렌식 조사 방법.

청구항 10

제 8 항에 있어서,

상기 행위 정보는,

하나의 양식으로 통일되어 데이터베이스 테이블에 입력되는 사용자 행위 분석을 위한 디지털 포렌식 조사 방법.

청구항 11

제 8 항에 있어서,

상기 분석 정보는,

상기 장치의 파일 시스템 정보, 레지스트리 정보, 이벤트 로그 정보, 프리페치 정보, 웹브라우저 정보, 로그 파일 정보 중 적어도 하나 이상을 포함하는 사용자 행위 분석을 위한 디지털 포렌식 조사 방법.

청구항 12

제 8 항에 있어서,

상기 행위 정보는,

응용 프로그램 설치, USB 저장장치 장착, 문서 사용, 프로그램 실행, 웹사이트 방문과 검색, 특정 시각의 파일 수정과 생성 중 적어도 하나 이상을 포함하는 사용자 행위 분석을 위한 디지털 포렌식 조사 방법.

청구항 13

제 11 항에 있어서,

상기 행위 정보를 파악하는 단계에서,

상기 분석 정보 중 레지스트리 정보를 수신하는 경우, 상기 레지스트리 정보의 분석을 통해 상기 장치에 USB 드라이브 장착이나 응용 프로그램 설치 여부를 판단하여 상기 사용자의 행위 정보로 파악하는 사용자 행위 분석을 위한 디지털 포렌식 조사 방법.

청구항 14

제 13 항에 있어서,

상기 행위 정보를 파악하는 단계에서,

상기 레지스트리 정보 중 MRU(most recently used) 킷값을 이용하여 상기 장치에서 문서 사용 여부를 판단하고, 이를 사용자의 행위 정보로 파악하는 사용자 행위 분석을 위한 디지털 포렌식 조사 방법.

명세서

기술 분야

[0001] 본 발명은 사용자 시스템에서의 디지털 조사 방법에 관한 것으로, 특히 컴퓨터 등 다양한 컴퓨팅 시스템(computing system)에서 사용자가 특정 시간에 무슨 행위를 하였는가를 알 수 있도록 사용자 행위 분석을 파악 수 있는 자료들을 수집 및 가공하여 시간 순서에 따라 조사자가 원하는 의미 있는 자료들을 수집하고, 수집된 자료들을 자동적으로 분석하여 시간 순서로 표시시켜줌으로서, 디지털 포렌식(digital forensic) 조사를 빠르고 효율적으로 할 수 있도록 하는 사용자 행위 분석을 위한 디지털 포렌식 장치 및 방법에 관한 것이다.

배경 기술

[0002] 일반적으로, 디지털 포렌식이란 디지털 증거를 수집하여 분석하는 기술이다. 이 디지털 포렌식은 증거의 수집, 보존, 분석, 문서화, 그리고 재판 과정에 증거로 제출하기까지의 모든 과정을 포함한다.

[0003] 최근 정보의 생산 및 유통에 있어서 디지털 형태의 정보가 약 95% 이상을 차지하고 있다. 디지털 기술의 발달로 범죄 증거는 네트워크(network), 인터넷(internet), 데이터베이스(data base), 모바일 장치 등 다양한 곳에서 존재한다. 휴대폰, PDA, 전자수첩, 디지털 카메라, MP3 플레이어, 캠코더, 휴대용 메모리 카드 등과 같은 휴대용 개인 디지털 장치는 작고 휴대가 용이하므로 범죄 증거의 은닉이 편리하다. 증거 확보의 필요성이 있는 경우, 이러한 개인 디지털 장치로부터 필요한 정보를 입수하여 분석하고 범죄 증거를 확보하는 것은 매우 중요하다.

[0004] 위와 같은, 디지털 포렌식 조사에서 컴퓨터 등의 장치를 대상으로 하여 분석을 진행할 때 다양한 정보들이 사용될 수 있고, 이러한 정보들을 획득하는데 사용하는 도구들은 여러 가지이다.

발명의 내용

해결하려는 과제

[0005] 하지만 실존하는 대부분의 디지털 포렌식 도구들은 다양한 정보를 제공하기는 하지만, 이렇게 제공된 정보들

은 단순히 수집된 대상이기 때문에 분석가가 이러한 정보를 모아서 의미 있는 자료를 만들기 위하여 한번 혹은 여러 번 가공하여야 하는 문제점이 있었다. 또한, 디지털 포렌식 조사 시에 발행되는 영장이 전체 디스크 이미징을 지원하지 않고, 특정 파일들만 수집할 수 있고 조사하는데 주어진 시간이 짧으면 여러 도구를 통하여 정보를 획득하고 가공하는 시간이 부족하게 되는 문제점이 있었다.

[0006] 따라서, 본 발명은 컴퓨터 등 다양한 컴퓨팅 시스템에서 사용자가 특정 시간에 무슨 행위를 하였는가를 알 수 있도록 사용자 행위 분석을 파악 수 있는 자료들을 수집 및 가공하여 시간 순서에 따라 조사자가 원하는 의미 있는 자료들을 수집하고, 수집된 자료들을 자동적으로 분석하여 시간 순서로 표시시켜줌으로서, 디지털 포렌식 조사를 빠르고 효율적으로 할 수 있도록 하는 사용자 행위 분석을 위한 디지털 포렌식 장치 및 방법을 제공하고자 한다.

과제의 해결 수단

[0007] 상술한 본 발명은 디지털 포렌식 장치로서, 사용자 행위 분석이 필요한 대상 장치로부터 사용자 행위와 관련된 분석 정보를 수집하는 수집부와, 상기 수집부로부터 수집되는 상기 분석 정보를 분석하여 각 분석 정보별 사용자의 행위 정보를 파악하고, 상기 행위 정보를 시간 순서대로 정렬하여 표시시키는 분석부를 포함한다.

[0008] 또한, 상기 수집부는, 상기 분석 정보 중 조사자에 의해 선택되는 분석 정보 항목을 입력받은 후, 상기 입력 받는 항목에 대한 분석 정보를 상기 장치로부터 수집하는 것을 특징으로 한다.

[0009] 또한, 상기 분석부는, 상기 행위 정보를 하나의 양식으로 통일하고 데이터베이스 테이블에 입력하는 것을 특징으로 한다.

[0010] 또한, 상기 분석 정보는, 상기 장치의 파일 시스템 정보, 레지스트리 정보, 이벤트 로그 정보, 프리페치 정보, 웹브라우저 정보, 로그파일 정보 중 적어도 하나 이상을 포함하는 것을 특징으로 한다.

[0011] 또한, 상기 분석부는, 상기 분석 정보 중 레지스트리 정보를 수신하는 경우, 상기 레지스트리 정보의 분석을 통해 상기 장치에 USB 드라이브 장착이나 응용 프로그램 설치 여부를 판단하여 상기 사용자의 행위 정보로 생성하는 것을 특징으로 한다.

[0012] 또한, 상기 분석부는, 상기 레지스트리 정보 중 MRU(most recently used) 킷값을 이용하여 상기 장치에서 문서 사용 여부를 판단하고, 이를 사용자의 행위 정보로 생성하는 것을 특징으로 한다.

[0013] 또한, 상기 행위 정보는, 응용 프로그램 설치, USB 저장장치 장착, 문서 사용, 프로그램 실행, 웹사이트 방문과 검색, 특정 시각의 파일 수정과 생성 중 적어도 하나 이상을 포함하는 것을 특징으로 한다.

[0014] 또한, 본 발명은 사용자 행위 분석을 위한 디지털 포렌식 조사 방법으로서, 사용자 행위 분석이 필요한 대상 장치로부터 사용자 행위와 관련된 분석 정보를 수집하는 단계와, 상기 수집한 분석 정보를 분석하여 각 분석 정보별 사용자의 행위 정보를 파악하는 단계와, 상기 행위 정보를 시간 순서대로 정렬하여 표시시키는 단계를 포함한다.

[0015] 또한, 상기 수집하는 단계는, 사용자 행위 분석이 필요한 대상 장치에 대해 수집할 분석 정보 항목을 입력받는 단계와, 상기 입력받은 항목에 대한 분석 정보를 상기 장치로부터 수집하는 단계를 포함하는 것을 특징으로 한다.

[0016] 또한, 상기 행위 정보는, 하나의 양식으로 통일되어 데이터베이스 테이블에 입력되는 것을 특징으로 한다.

[0017] 또한, 상기 분석 정보는, 상기 장치의 파일 시스템 정보, 레지스트리 정보, 이벤트 로그 정보, 프리페치 정보, 웹브라우저 정보, 로그파일 정보 중 적어도 하나 이상을 포함하는 것을 특징으로 한다.

[0018] 또한, 상기 행위 정보는, 응용 프로그램 설치, USB 저장장치 장착, 문서 사용, 프로그램 실행, 웹사이트 방문과 검색, 특정 시각의 파일 수정과 생성 중 적어도 하나 이상을 포함하는 것을 특징으로 한다.

[0019] 또한, 상기 행위 정보를 파악하는 단계에서, 상기 분석 정보 중 레지스트리 정보를 수신하는 경우, 상기 레지스트리 정보의 분석을 통해 상기 장치에 USB 드라이브 장착이나 응용 프로그램 설치 여부를 판단하여 상기 사용자의 행위 정보로 파악하는 것을 특징으로 한다.

[0020] 또한, 상기 행위 정보를 파악하는 단계에서, 상기 레지스트리 정보 중 MRU(most recently used) 킷값을 이용

하여 상기 장치에서 문서 사용 여부를 판단하고, 이를 사용자의 행위 정보로 파악하는 것을 특징으로 한다.

발명의 효과

- [0021] 본 발명에서는 컴퓨터 등 다양한 컴퓨팅 시스템에서 사용자가 특정 시간에 무슨 행위를 하였는가를 알 수 있도록 사용자 행위 분석을 파악 수 있는 자료들을 수집 및 가공하여 시간 순서에 따라 조사자가 원하는 의미 있는 자료들을 수집하고, 수집된 자료들을 자동적으로 분석하여 시간 순서로 표시시켜줌으로서, 디지털 포렌식 조사를 빠르고 효율적으로 수행할 수 있는 이점이 있다.
- [0022] 또한, 본 발명에서와 같이 특정 시스템에서 사용자의 행위에 대해 시간 순서대로 표시하여줌으로써 조사자가 특정 시간대에 일어난 일들을 상세하면서도 쉽게 인지할 수 있으며, 여러 도구를 사용하여 수집을 하지 않고 하나의 도구로 분석을 수행할 수 있기 때문에 조사시간을 상당히 줄일 수 있는 이점이 있다.

도면의 간단한 설명

- [0023] 도 1은 본 발명의 실시 예에 따른 디지털 포렌식 장치의 블록 구성도,
 도 2는 본 발명의 실시 예에 따른 분석 정보와 행위 정보 예시도,
 도 3은 본 발명의 실시 예에 따른 디지털 포렌식 장치에서 사용자 행위 분석을 위한 포렌식 조사 흐름도.

발명을 실시하기 위한 구체적인 내용

- [0024] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시 예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시 예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시 예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.
- [0025] 본 발명의 실시 예들을 설명함에 있어서 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이며, 후술되는 용어들은 본 발명의 실시 예에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.
- [0026] 첨부된 블록도의 각 블록과 흐름도의 각 단계의 조합들은 컴퓨터 프로그램 인스트럭션들(실행 엔진)에 의해 수행될 수도 있으며, 이들 컴퓨터 프로그램 인스트럭션들은 범용 컴퓨터, 특수용 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서에 탑재될 수 있으므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서를 통해 수행되는 그 인스트럭션들이 블록도의 각 블록 또는 흐름도의 각 단계에서 설명된 기능들을 수행하는 수단을 생성하게 된다. 이들 컴퓨터 프로그램 인스트럭션들은 특정 방식으로 기능을 구현하기 위해 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 지향할 수 있는 컴퓨터 이용 가능 또는 컴퓨터 판독 가능 메모리에 저장되는 것도 가능하므로, 그 컴퓨터 이용가능 또는 컴퓨터 판독 가능 메모리에 저장된 인스트럭션들은 블록도의 각 블록 또는 흐름도의 각 단계에서 설명된 기능을 수행하는 인스트럭션 수단을 내포하는 제조 품목을 생산하는 것도 가능하다.
- [0027] 그리고, 컴퓨터 프로그램 인스트럭션들은 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에 탑재되는 것도 가능하므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에서 일련의 동작 단계들이 수행되어 컴퓨터로 실행되는 프로세스를 생성해서 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 수행하는 인스트럭션들은 블록도의 각 블록 및 흐름도의 각 단계에서 설명되는 기능들을 실행하기 위한 단계들을 제공하는 것도 가능하다.
- [0028] 또한, 각 블록 또는 각 단계는 특정된 논리적 기능들을 실행하기 위한 하나 이상의 실행 가능한 인스트럭션들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있으며, 몇 가지 대체 실시 예들에서는 블록들 또는 단계들에서 언급된 기능들이 순서를 벗어나서 발생하는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들 또는 단계들은 사실 실질적으로 동시에 수행되는 것도 가능하며, 또한 그 블록들

또는 단계들이 필요에 따라 해당하는 기능의 역순으로 수행되는 것도 가능하다.

- [0029] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시 예에 대하여 상세하게 설명한다.
- [0030] 도 1은 본 발명의 실시 예에 따른 디지털 포렌식 장치(100)의 상세 블록 구성을 도시한 것이다.
- [0031] 도 1을 참조하면, 수집부(102)는 사용자의 행위를 파악하기 위한 대상 컴퓨터 시스템 등으로부터 사용자의 행위와 관련된 정보를 수집한다. 이와 같은 정보는 도 2에 도시된 바와 같이, 분석 정보와 행위 정보 등으로 구분될 수 있다.
- [0032] 분석 정보는 사용자의 행위에 따라 컴퓨터 등의 시스템에 기록되는 정보로, 예를 들어, 레지스트리(registry), 특별한 폴더(specific folder), 이벤트 로그(event log), 프리페치(prefetch), 웹 히스토리(web history), 웹 브라우저(web browser), 메모리(memory), 파일 시스템(file system), 기타 로그 파일(log file) 등의 정보를 의미한다.
- [0033] 행위 정보는 분석 정보에 포함되는 컴퓨터 시스템의 각 시스템 정보가 의미하는 구체적인 행위 정보를 나타내는 것으로, 예를 들어, 레지스트리 정보로부터는 응용 프로그램 설치, USB 저장장치 장착, 문서 사용 등의 사용자의 행위를 파악할 수 있다.
- [0034] 또한, 특별한 폴더(specific folder) 정보로부터는 문서 사용 등의 행위, 프리페치 정보로부터는 프로그램 실행 등의 행위, 이벤트 로그 정보로부터는 컴퓨터 시작/종료 등의 행위를 파악할 수 있다. 또한, 웹 히스토리 정보로부터는 웹사이트 방문/검색 등의 행위, 파일 시스템 정보로부터는 특정 시각의 수정/생성 파일 등의 행위를 파악할 수 있다.
- [0035] 이하, 분석 정보의 각 항목에 대한 사용자의 행위 파악에 대해 보다 상세히 설명하기로 한다.
- [0036] 먼저, 레지스트리는 사용자 계정, 컴퓨터의 하드웨어(hardware), 소프트웨어(software) 등에 대한 구성 정보가 담긴 계층적인 트리 구조(tree structure)의 데이터베이스(database)이다. 레지스트리는 USB 드라이브 장착 정보나 응용프로그램 설치정보와 같은 사용자 행위에 의해 생성된 정보를 포함하고 있기 때문에 디지털 포렌식 조사에 활용할 수 있는 충분한 가치를 가지고 있는 자료이다. 단, 레지스트리는 최종수정시각(LastWriteTime)만을 기록하게 되어 있으며, UTC Time으로 기록하는 점을 분석 시 고려하여 적절히 가공해주어야 한다.
- [0037] USB 저장장치는 기업 기반 시스템의 보안에 위협이 될 수 있으며, 최근 들어 크기는 줄어들면서 저장 용량은 커져 더 많은 문서자료, 프리젠테이션(presentation) 자료를 저장 할 수 있게 되었다. 또한, 시스템이 악성코드에 감염되었을 경우 USB 저장장치의 고유한 인스턴스(instance) 값을 확인하여 감염 매체나 감염 방법을 확인할 수 있다. 이러한 USB 저장장치의 정보 및 장착 시간은 사용자 행위 분석에 필요한 자료 조사에 중요한 요소로 활용할 수 있다.
- [0038] USB 저장장치 장착정보는 레지스트리의 시스템 파일에 존재하며, USB 저장장치에 해당하는 키(key) 값을 이용하여 최종수정시각(LastWriteTime)을 통해 부팅 후 장착되었던 USB 저장장치 정보를 획득 할 수 있다.
- [0039] 응용 프로그램은 설치 시 자신의 실행 경로와 실행 파일은 레지스트리의 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths의 하위 키에 등록된다. 이 키 값 정보를 이용하여 시스템에 설치되어 있는 응용프로그램 목록을 획득할 수 있다.
- [0040] App Paths의 전체 하위 키를 조사함으로써 시스템에 설치된 모든 응용프로그램과 그에 해당하는 실행파일의 경로 정보를 알 수 있으며, 각 키의 최종수정시각(LastWriteTime)을 통하여 응용프로그램의 설치시각을 알 수 있다. 또한 이 정보들을 활용하면 응용프로그램이 설치된 시간을 기준으로 목록을 구성할 수 있다. 특정 시각에 어떠한 응용프로그램을 설치하였으나, 조사 시에 그 응용프로그램이 존재하지 않으면 사용 후 삭제하였음을 짐작 할 수 있다. 특히 안티 포렌식 도구를 사용하고 난 뒤 삭제를 하였다면, 의도적으로 악의적인 행동을 했음을 유추 할 수 있다.
- [0041] 윈도우즈 XP 이후 버전부터 존재하는 프리페치(prefetch) 파일은 응용프로그램의 실행 속도 향상을 위해 응용프로그램 구동에 필요한 자료를 미리 메모리에 올리는 기술이다.
- [0042] 프리페치 정보를 이용하면 최근에 실행된 파일의 최근 실행 시각, 경로 및 총 실행 횟수 등을 알 수 있다. 실행 파일의 전체 경로를 알고 있으면 파일의 MAC(Modified, Accessed, Created) 시간을 알 수 있다. 파일의 생성시각 정보는 언제 실행파일이 만들어 졌는지를 알 수 있다. 이러한 파일의 실행시각, 생성시각은 특정 시간

에 일어난 행위를 분석하는데 활용할 수 있다.

- [0043] '%windir%\prefetch' 폴더에 [파일이름]-[HASH].pf 으로 이루어진 파일이 존재하며 응용프로그램의 총 실행 횟수, 마지막 실행 시각, 참조한 라이브러리 정보 등을 담고 있다. 윈도우즈 구동 시 기본적으로 실행되는 서비스인 WMIPRVSE.EXE, WUAUCLT.EXE의 파일 실행시각은 윈도우즈 시스템 구동 시각과 일치하기 때문에 위의 두 파일의 실행시각을 사용하여 시스템 구동 시각을 파악할 수 있다.
- [0044] 사용자 행위 분석관점에서 필요한 이벤트 로그중의 내용은 사용자가 컴퓨터 사용을 시작한 시각, 컴퓨터 사용을 종료한 시각이다. 이러한 정보는 사용자 행위 분석의 기준으로 활용 할 수 있다.
- [0045] 윈도우즈는 시스템 경고나 오류 보고, 감사 정책과 관련된 로그를 이벤트 로그에 기록하고 있다. 윈도우즈 시스템은 응용프로그램 로그, 보안 로그, 시스템 로그와 같은 세 가지 로그를 이벤트에 기록 한다.
- [0046] 대부분의 사용자들의 PC 사용목적은 웹 브라우저를 이용한 인터넷 서핑이다. 그렇기 때문에 웹 브라우저의 사용내역도 포렌식 조사 시 매우 중요한 분야이다. 현존하는 대부분의 웹 브라우저들은 빠른 속도를 보장하기 위해 웹 브라우저가 설치된 시스템 내부에 캐쉬파일(cache file), 쿠키파일(cookie file), 방문기록, 다운로드 받은 파일과 같은 여러 정보 파일을 생성 및 보관하고 있다.
- [0047] 한편, 윈도우즈 XP 이후 버전부터 제공되고 있는 기능으로써, 최근에 사용한 문서에 대한 정보를 제공하여 준다. 크게 최근 사용 문서에 대한 정보를 얻는 방법은 두 가지로 나뉘어진다.
- [0048] 첫 번째로는 레지스트리의 MRU(Most Recently Used)키 값을 사용하는 방법이다. XP 기준의 레지스트리 주소는 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU 이다. 이 키 값을 통하여 사용한 문서 파일의 확장자 별로 정보를 획득 할 수 있다.
- [0049] 두 번째 방법으로는 %USERPROFILE%\Recent 폴더의 링크파일을 이용하는 방법이 있다.
- [0050] 위의 두 가지 방법으로 획득한 최근 사용 문서 파일에 대한 정보를 통하여 사용자의 작업 행동을 파악할 수 있다. 특히 한글이나 MS Word 파일과 같이 자주 사용되는 문서 파일들은 중요한 자료가 될 수 있다. 문서파일이 마지막으로 수정된 시각을 알 수 있고, 이를 통하여 문서 작업 내역의 흐름을 확인할 수 있다. 또한 최근 문서 내역에는 존재하지만 실제로 파일이 존재하지 않으면 작업 후에 USB 저장소로 옮기거나 삭제했다고 추측할 수 있기 때문에 포렌식 조사에 유용한 정보로 사용할 수 있다.
- [0051] 분석부(104)는 사용자의 행위 파악이 필요한 대상 컴퓨터 시스템 등에 대해 위와 같이 수집부로부터 포렌식 조사 시에 여러 도구를 통해 각 도구에서 획득할 수 있는 자료들을 수집한다. 또한, 분석부(104)는 위와 같이 수집된 자료들에 대해 분석 정보를 분석하여 각 분석 정보별 사용자의 행위 정보를 파악한다. 이어, 이와 같이 파악한 사용자의 행위 정보에 대해 표시부(106)를 통해 표시시켜 조사자가 시각적으로 표현된 자료를 통하여 좀 더 빠르고 효율적인 조사를 진행할 수 있도록 한다.
- [0052] 한편, 분석부(104)는 위와 같이 분석된 사용자의 행위를 표시부(106)상 시간순으로 열거하여 표시시킬 수 있는데, 사용자의 행위를 시간 순으로 열거하면 사건을 흐름별로 추측할 수 있다. 또한, 분석된 사용자의 행위를 열거만 하는 것이 아니라 표시부(106)를 통해 표시시키는 것과 같이 시각화를 하여주면 한눈에 사용자가 어떤 행위를 하였는지 쉽게 알 수 있다.
- [0053] 도 3은 본 발명의 실시 예에 따른 디지털 포렌식 장치(100)에서 사용자의 행위를 파악하는 동작 제어 흐름을 도시한 것이다. 이하, 도 1 내지 도 3을 참조하여 본 발명의 실시 예를 상세히 설명하기로 한다.
- [0054] 먼저, 사용자의 행위를 파악하기 위한 대상 컴퓨터 시스템 등에 대해 조사자는 사용자의 행위와 관련된 정보 중 수집부(102)를 통해 수집하고자 하는 항목을 선택한다(S300).
- [0055] 이에 따라, 수집부(102)는 조사자에 의해 선택된 분석 항목 정보를 인지하여, 컴퓨터 시스템내 사용자의 행위와 관련되는 저장되는 다양한 정보 중 조사자에 의해 선택된 분석 정보를 수집한다(S302).
- [0056] 이때, 분석 정보를 전술한 바와 같이, 레지스트리, 특별한 폴더, 프리페치, 이벤트 로그, 웹 히스토리, 파일 시스템 등의 정보가 될 수 있으며, 이와 같은 분석 정보 중 조사자에 의해 선택된 항목의 분석 정보를 수집하여 시간 순으로 정렬시킨다.
- [0057] 위와 같이, 시간 순으로 정렬되어 수집된 정보는 분석부(104)로 인가된다. 그러면, 분석부(104)는 수집부(102)로부터 수집된 분석 정보를 시간 순으로 정렬하고(S304), 각 분석 정보에 대응하는 사용자의 행위 정보를 파악하여 파악된 다양한 행위 정보를 하나의 양식으로 통일시킨다(S306).

[0058] 이어, 분석부(104)는 통일된 양식의 자료를 하나의 데이터베이스 테이블(database table)에 입력하고(S308), 각 항목별 병합된 자료를 시간 순으로 표시부(106)상에 표시시킴으로써 조사자가 특정 컴퓨터 등의 시스템에서 사용자들의 행위를 보다 쉽게 확인할 수 있도록 한다(S310).

[0059] 상술한 바와 같이, 본 발명은 컴퓨터 등 다양한 컴퓨팅 시스템에서 사용자가 특정 시간에 무슨 행위를 하였는가를 알 수 있도록 사용자 행위 분석을 파악할 수 있는 자료들을 수집 및 가공하여 시간 순서에 따라 조사자가 원하는 의미 있는 자료들을 수집하고, 수집된 자료들을 자동적으로 분석하여 시간 순서로 표시시켜줌으로서, 디지털 포렌식 조사를 빠르고 효율적으로 수행할 수 있다. 또한, 특정 시스템에서 사용자의 행위에 대해 시간 순서대로 표시하여줌으로써 조사자가 특정 시간대에 일어난 일들을 상세하면서도 쉽게 인지할 수 있으며, 여러 도구를 사용하여 수집을 하지 않고 하나의 도구로 분석을 수행할 수 있기 때문에 조사시간을 상당히 줄일 수 있다.

[0060] 한편 상술한 본 발명의 설명에서는 구체적인 실시 예에 관해 설명하였으나, 여러 가지 변형이 본 발명의 범위에서 벗어나지 않고 실시될 수 있다. 따라서 발명의 범위는 설명된 실시 예에 의하여 정할 것이 아니고 특허 청구범위에 의해 정하여져야 한다.

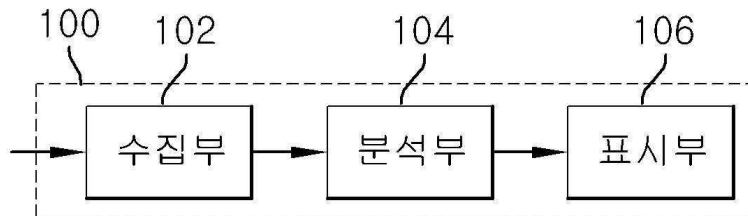
부호의 설명

[0061] 100 : 수집부 102 : 분석부

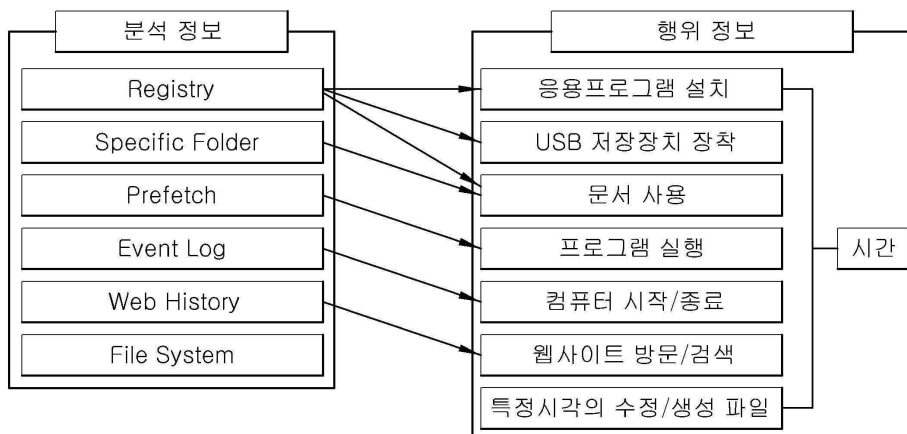
104 : 표시부

도면

도면1



도면2



도면3

