(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년11월27일
(11) 등록번호 10-2049455
(24) 등록일자 2019년11월21일

(51) 국제특허분류(Int. Cl.)
G06F 21/60 (2013.01) *G06F 16/11* (2019.01)
G06F 21/71 (2013.01)
(52) CPC특허분류
G06F 21/60 (2013.01)
G06F 16/119 (2019.01)
(21) 출원번호 10-2019-0064254
(22) 출원일자 2019년05월31일
심사청구일자 2019년05월31일
(56) 선행기술조사문헌
KR101497067 B1*
KR1020190033381 A*
US20070067600 A1*
KR1020090001457 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
대한민국

(72) 발명자
성기범
경기도 안양시 동안구 XXXXXXXXXXX XXXXXX

(74) 대리인
김광호

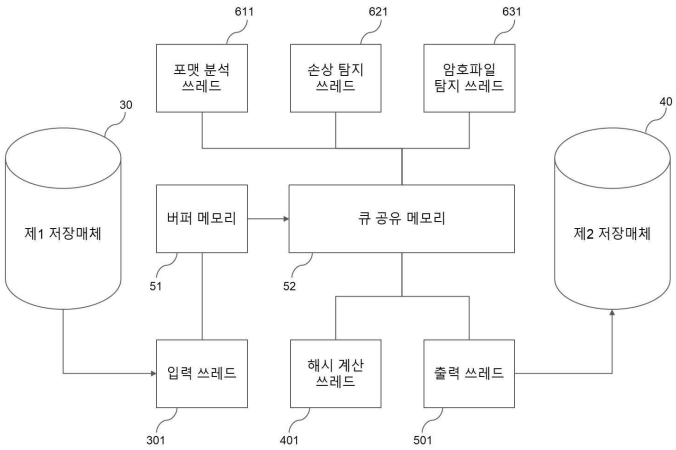
전체 청구항 수 : 총 16 항 심사관 : 구대성

(54) 발명의 명칭 **디지털 포렌식 기반의 대용량 전자기록물 이관 시스템 및 방법**

(57) 요 약

제1 저장매체에 저장된 파일들 중 적어도 하나 이상의 파일의 속성 정보를 포함하는 이관 대상 파일 목록을 생성하는 파일 목록 생성부, 병렬 처리되는 입력 쓰레드, 해시 계산 쓰레드 및 출력 쓰레드 중 적어도 하나 이상을 생성하는 쓰레드 생성부, 상기 입력 쓰레드를 이용하여, 상기 제1 저장매체에 저장된 파일들 중 상기 이관 대상 파일 목록에 포함된 파일을 읽어 메모리에 저장하는 파일 입력부, 상기 해시 계산 쓰레드를 이용하여, 상기 메모리에 저장된 파일의 해시값을 계산하는 해시 계산부, 상기 출력 쓰레드를 이용하여, 상기 메모리에 저장된 파일을 제2 저장매체에 저장하는 파일 출력부 및 상기 제2 저장매체에 저장된 파일 각각의 속성 정보 및 상기 시값을 포함하는 수집 목록 파일을 생성하는 결과 출력부를 포함하는, 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템.

대 표 도 - 도5



(52) CPC특허분류
G06F 16/122 (2019.01)
G06F 21/71 (2013.01)

명 세 서

청구범위

청구항 1

제1 저장매체에 저장된 파일들 중 적어도 하나 이상의 파일의 속성 정보를 포함하는 이관 대상 파일 목록을 생성하는 파일 목록 생성부;

병렬 처리되는 입력 쓰레드, 해시 계산 쓰레드 및 출력 쓰레드 중 적어도 하나 이상을 생성하는 쓰레드 생성부;

상기 입력 쓰레드를 이용하여, 상기 제1 저장매체에 저장된 파일들 중 상기 이관 대상 파일 목록에 포함된 파일을 읽어 메모리에 저장하는 파일 입력부;

상기 해시 계산 쓰레드를 이용하여, 상기 메모리에 저장된 파일의 해시값을 계산하는 해시 계산부;

상기 출력 쓰레드를 이용하여, 상기 메모리에 저장된 파일을 제2 저장매체에 저장하는 파일 출력부; 및

상기 제2 저장매체에 저장된 파일 각각의 속성 정보 및 상기 해시값을 포함하는 수집 목록 파일을 생성하는 결과 출력부;를 포함하되,

포맷 분석 쓰레드를 이용하여, 상기 메모리에 저장된 파일의 확장자가 파일의 형식과 일치하는지 분석하는 포맷 분석부;를 더 포함하고,

상기 쓰레드 생성부는 상기 입력 쓰레드, 상기 해시 계산 쓰레드 및 상기 출력 쓰레드와 병렬 처리되는 상기 포맷 분석 쓰레드를 더 생성하며,

상기 수집 목록 파일은 상기 포맷 분석부의 분석 결과를 더 포함하는, 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템.

청구항 2

삭제

청구항 3

제1항에 있어서,

손상 탐지 쓰레드를 이용하여, 상기 메모리에 저장된 파일이 손상되었는지를 탐지하는 손상 탐지부;를 더 포함하고,

상기 쓰레드 생성부는 상기 입력 쓰레드, 상기 해시 계산 쓰레드 및 상기 출력 쓰레드와 병렬 처리되는 상기 손상 탐지 쓰레드를 더 생성하며,

상기 수집 목록 파일은 상기 손상 탐지부의 탐지 결과를 더 포함하는 것을 특징으로 하는, 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템.

청구항 4

제1항에 있어서,

암호파일 탐지 쓰레드를 이용하여, 상기 메모리에 저장된 파일에 암호가 설정되어 있는지를 탐지하는 암호파일 탐지부;를 더 포함하고,

상기 쓰레드 생성부는 상기 입력 쓰레드, 상기 해시 계산 쓰레드 및 상기 출력 쓰레드와 병렬 처리되는 상기 암호파일 탐지 쓰레드를 더 생성하며,

상기 수집 목록 파일은 상기 암호파일 탐지부의 탐지 결과를 더 포함하는 것을 특징으로 하는, 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템.

청구항 5

제1항에 있어서,

상기 메모리는 서로 다른 사이즈들로 사전 선언된 버퍼 메모리들을 포함하고,

상기 파일 입력부는 상기 사전 선언된 버퍼 메모리들 중 읽어 들일 파일의 크기에 대응되는 버퍼 메모리를 동적으로 할당받아 파일 읽기 동작을 수행하는 것을 특징으로 하는, 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템.

청구항 6

제5항에 있어서,

상기 파일 입력부는 상기 사전 선언된 버퍼 메모리들 중 읽어 들일 파일의 크기에 대응되는 버퍼 메모리가 없는 경우 가장 큰 사이즈의 버퍼 메모리를 복수회 이용하여 파일 읽기 동작을 수행하는 것을 특징으로 하는, 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템.

청구항 7

제1항에 있어서,

상기 제2 저장매체에 저장된 파일의 해시값은 상기 제1 저장매체에 저장된 파일의 해시값과 동일한 것을 특징으로 하는, 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템.

청구항 8

제1항에 있어서,

상기 제2 저장매체에 저장된 파일의 생성 시간, 수정 시간 및 접근 시간은 각각 상기 제1 저장매체에 저장된 파일의 생성 시간, 수정 시간 및 접근 시간과 동일한 것을 특징으로 하는, 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템.

청구항 9

제1항에 있어서,

상기 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템은

상기 파일 목록 생성부, 상기 쓰레드 생성부, 상기 파일 입력부, 상기 해시 계산부, 상기 파일 출력부 및 상기 결과 출력부를 포함하는 이관도구; 및 상기 제2 저장매체와 같거나 다른 제3 저장매체에 상기 이관도구를 설치하는 배포기로 구성되며,

상기 이관도구는 상기 배포기에 의해 설치된 상기 제3 저장매체에서만 실행되는 것을 특징으로 하는, 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템.

청구항 10

제1 저장매체에 저장된 파일들 중 적어도 하나 이상의 파일의 속성 정보를 포함하는 이관 대상 파일 목록을 생성하는 파일 목록 생성 단계;

병렬 처리되는 입력 쓰레드, 해시 계산 쓰레드 및 출력 쓰레드 중 적어도 하나 이상을 생성하는 쓰레드 생성 단계;

상기 입력 쓰레드를 이용하여, 상기 제1 저장매체에 저장된 파일들 중 상기 이관 대상 파일 목록에 포함된 파일을 읽어 메모리에 저장하는 파일 입력 단계;

상기 해시 계산 쓰레드를 이용하여, 상기 메모리에 저장된 파일의 해시값을 계산하는 해시 계산 단계;

상기 출력 쓰레드를 이용하여, 상기 메모리에 저장된 파일을 제2 저장매체에 저장하는 파일 출력 단계; 및

상기 제2 저장매체에 저장된 파일 각각의 속성 정보 및 상기 해시값을 포함하는 수집 목록 파일을 생성하는 결과 출력 단계;를 포함하되,

포맷 분석 쓰레드를 이용하여, 상기 메모리에 저장된 파일의 확장자가 파일의 형식과 일치하는지 분석하는 포맷 분석 단계;를 더 포함하고,

상기 쓰레드 생성 단계는 상기 입력 쓰레드, 상기 해시 계산 쓰레드 및 상기 출력 쓰레드와 병렬 처리되는 상기 포맷 분석 쓰레드를 더 생성하며,

상기 수집 목록 파일은 상기 포맷 분석 단계에서 분석된 결과를 더 포함하는, 디지털 포렌식 기반의 대용량 전자기록물 이관 방법.

청구항 11

삭제

청구항 12

제10항에 있어서,

손상 탐지 쓰레드를 이용하여, 상기 메모리에 저장된 파일이 손상되었는지를 탐지하는 손상 탐지 단계;를 더 포함하고,

상기 쓰레드 생성 단계는 상기 입력 쓰레드, 상기 해시 계산 쓰레드 및 상기 출력 쓰레드와 병렬 처리되는 상기 손상 탐지 쓰레드를 더 생성하며,

상기 수집 목록 파일은 상기 손상 탐지 단계에서 탐지된 결과를 더 포함하는 것을 특징으로 하는, 디지털 포렌식 기반의 대용량 전자기록물 이관 방법.

청구항 13

제10항에 있어서,

암호파일 탐지 쓰레드를 이용하여, 상기 메모리에 저장된 파일에 암호가 설정되어 있는지를 탐지하는 암호파일 탐지 단계;를 더 포함하고,

상기 쓰레드 생성 단계는 상기 입력 쓰레드, 상기 해시 계산 쓰레드 및 상기 출력 쓰레드와 병렬 처리되는 상기 암호파일 탐지 쓰레드를 더 생성하며,

상기 수집 목록 파일은 상기 암호파일 탐지 단계에서 탐지된 결과를 더 포함하는 것을 특징으로 하는, 디지털 포렌식 기반의 대용량 전자기록물 이관 방법.

청구항 14

제10항에 있어서,

상기 메모리는 서로 다른 사이즈들로 사전 선언된 버퍼 메모리들을 포함하고,

상기 파일 입력 단계는 상기 사전 선언된 버퍼 메모리들 중 읽어 들일 파일의 크기에 대응되는 버퍼 메모리를 동적으로 할당받아 파일 읽기 동작을 수행하는 것을 특징으로 하는, 디지털 포렌식 기반의 대용량 전자기록물 이관 방법.

청구항 15

제14항에 있어서,

상기 파일 입력 단계는 상기 사전 선언된 버퍼 메모리들 중 읽어 들일 파일의 크기에 대응되는 버퍼 메모리가 없는 경우 가장 큰 사이즈의 버퍼 메모리를 복수회 이용하여 파일 읽기 동작을 수행하는 것을 특징으로 하는, 디지털 포렌식 기반의 대용량 전자기록물 이관 방법.

청구항 16

제10항에 있어서,

상기 제2 저장매체에 저장된 파일의 해시값은 상기 제1 저장매체에 저장된 파일의 해시값과 동일한 것을 특징으로 하는, 디지털 포렌식 기반의 대용량 전자기록물 이관 방법.

청구항 17

제10항에 있어서,

상기 제2 저장매체에 저장된 파일의 생성 시간, 수정 시간 및 접근 시간은 각각 상기 제1 저장매체에 저장된 파일의 생성 시간, 수정 시간 및 접근 시간과 동일한 것을 특징으로 하는, 디지털 포렌식 기반의 대용량 전자기록물 이관 방법.

청구항 18

제10항에 있어서,

상기 파일 목록 생성 단계, 상기 쓰레드 생성 단계, 상기 파일 입력 단계, 상기 해시 계산 단계, 상기 파일 출력 단계 및 상기 결과 출력 단계를 실행시키기 위한 이관도구 프로그램을 상기 제2 저장매체와 같거나 다른 제3 저장매체에 설치하는 배포 단계;를 더 포함하고,

상기 이관도구 프로그램은 상기 배포 단계에서 설치된 상기 제3 저장매체에서만 실행되는 것을 특징으로 하는, 디지털 포렌식 기반의 대용량 전자기록물 이관 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템 및 방법에 관한 것으로, 더욱 상세하게는 병렬처리되는 복수의 쓰레드를 통해 파일을 입력 및 출력하고, 해시값을 계산하여 이관 속도를 향상시킬 수 있는 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 전자기록물이란 정부의 각 기관에서 업무수행을 위해 컴퓨터시스템을 이용하여 전자포맷으로 생성, 유통, 관리하는 모든 기록물로서 각 기관의 활동에 대한 증거물 역할을 한다.

[0003] 일반적으로 전자기록물은 하드디스크, USB 등의 저장매체를 사용하여 오프라인으로 이관되거나, 각 기관 간에 연결된 네트워크를 통해 온라인으로 이관되며, 전자기록물은 디지털 데이터의 일종이기 때문에 특성상 이관 과정에서 데이터의 조작, 변경, 삭제의 위험에 노출되어 있다.

[0004] 특히, 점차 대용량화 되어가는 IT환경에서 전자기록물의 이관과 관련하여 진본성, 무결성, 신뢰성 및 이용가능성이 보장되어야 하며, 이러한 전자기록물 이관의 4대 속성을 보장하기 위하여 디지털 포렌식(Digital Forensic) 기법이 활용되고 있다.

[0005] 디지털 포렌식 기법이란 컴퓨터 시스템에서 자료를 수집하는 단계에서부터 이를 분석하고 분석된 자료에 대한 보고서를 작성하며 수집된 증거물의 원본 일치성을 보증하는 일련의 과정을 말한다. 이러한 디지털 포렌식은 하드디스크나 USB와 같은 저장매체에 저장된 디지털 자료에 대해 컴퓨터를 이용하여 일어난 어떤 행위의 사실관계를 규명하고 증명하는 기법이다.

[0006] 전자기록물 이관에 디지털 포렌식 기법을 적용하기 위해서 해시값이 사용되고 있으며, 해시값의 비교를 통해 파일의 조작 내지는 변경 여부를 확인할 수 있다. 또한, 이관 과정에서 발생할 수 있는 오류 내지는 중단을 예방하고, 이관의 4대 속성을 보장하기 위하여 파일에 대한 검사 내지는 분석이 수행될 수 있다.

[0007] 대용량/대량 전자기록물 이관에 있어서 이러한 해시값의 계산 및 파일에 대한 검사/분석은 이관 속도를 저하시키는 문제점으로 작용하고 있다.

발명의 내용

해결하려는 과제

[0008] 이에, 본 발명의 기술적 과제는 이러한 점에서 착안된 것으로 본 발명의 목적은 이관 과정에서 파일에 대한 해

시값의 계산, 검사 및 분석 과정을 쓰레드를 이용하여 병렬 처리함으로서 이관 속도를 향상시킬 수 있는 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템 및 방법을 제공하는 것이다.

과제의 해결 수단

[0009] 상기한 본 발명의 목적을 실현하기 위한 일 실시예에 따른, 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템은 제1 저장매체에 저장된 파일들 중 적어도 하나 이상의 파일의 속성 정보를 포함하는 이관 대상 파일 목록을 생성하는 파일 목록 생성부; 병렬 처리되는 입력 쓰레드, 해시 계산 쓰레드 및 출력 쓰레드 중 적어도 하나 이상을 생성하는 쓰레드 생성부; 상기 입력 쓰레드를 이용하여, 상기 제1 저장매체에 저장된 파일들 중 상기 이관 대상 파일 목록에 포함된 파일을 읽어 메모리에 저장하는 파일 입력부; 상기 해시 계산 쓰레드를 이용하여, 상기 메모리에 저장된 파일의 해시값을 계산하는 해시 계산부; 상기 출력 쓰레드를 이용하여, 상기 메모리에 저장된 파일을 제2 저장매체에 저장하는 파일 출력부; 및 상기 제2 저장매체에 저장된 파일 각각의 속성 정보 및 상기 해시값을 포함하는 수집 목록 파일을 생성하는 결과 출력부;를 포함한다.

[0010] 본 발명의 일 실시예에 있어서, 포맷 분석 쓰레드를 이용하여, 상기 메모리에 저장된 파일의 확장자가 파일의 형식과 일치하는지 분석하는 포맷 분석부;를 더 포함하고, 상기 쓰레드 생성부는 상기 입력 쓰레드, 상기 해시 계산 쓰레드 및 상기 출력 쓰레드와 병렬 처리되는 상기 포맷 분석 쓰레드를 더 생성하며, 상기 수집 목록 파일은 상기 포맷 분석부의 분석 결과를 더 포함할 수 있다.

[0011] 본 발명의 일 실시예에 있어서, 손상 탐지 쓰레드를 이용하여, 상기 메모리에 저장된 파일이 손상되었는지를 탐지하는 손상 탐지부;를 더 포함하고, 상기 쓰레드 생성부는 상기 입력 쓰레드, 상기 해시 계산 쓰레드 및 상기 출력 쓰레드와 병렬 처리되는 상기 손상 탐지 쓰레드를 더 생성하며, 상기 수집 목록 파일은 상기 손상 탐지부의 탐지 결과를 더 포함할 수 있다.

[0012] 본 발명의 일 실시예에 있어서, 암호파일 탐지 쓰레드를 이용하여, 상기 메모리에 저장된 파일에 암호가 설정되어 있는지를 탐지하는 암호파일 탐지부;를 더 포함하고, 상기 쓰레드 생성부는 상기 입력 쓰레드, 상기 해시 계산 쓰레드 및 상기 출력 쓰레드와 병렬 처리되는 상기 암호파일 탐지 쓰레드를 더 생성하며, 상기 수집 목록 파일은 상기 암호파일 탐지부의 탐지 결과를 더 포함할 수 있다.

[0013] 본 발명의 일 실시예에 있어서, 상기 메모리는 서로 다른 사이즈들로 사전 선언된 버퍼 메모리들을 포함하고, 상기 파일 입력부는 상기 사전 선언된 버퍼 메모리들 중 읽어 들일 파일의 크기에 대응되는 버퍼 메모리를 동적으로 할당받아 파일 읽기 동작을 수행할 수 있다.

[0014] 본 발명의 일 실시예에 있어서, 상기 파일 입력부는 상기 사전 선언된 버퍼 메모리들 중 읽어 들일 파일의 크기에 대응되는 버퍼 메모리가 없는 경우 가장 큰 사이즈의 버퍼 메모리를 복수회 이용하여 파일 읽기 동작을 수행할 수 있다.

[0015] 본 발명의 일 실시예에 있어서, 상기 제2 저장매체에 저장된 파일의 해시값은 상기 제1 저장매체에 저장된 파일의 해시값과 동일할 수 있다.

[0016] 본 발명의 일 실시예에 있어서, 상기 제2 저장매체에 저장된 파일의 생성 시간, 수정 시간 및 접근 시간은 각각 상기 제1 저장매체에 저장된 파일의 생성 시간, 수정 시간 및 접근 시간과 동일할 수 있다.

[0017] 본 발명의 일 실시예에 있어서, 상기 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템은 상기 파일 목록 생성부, 상기 쓰레드 생성부, 상기 파일 입력부, 상기 해시 계산부, 상기 파일 출력부 및 상기 결과 출력부를 포함하는 이관도구; 및 상기 제2 저장매체와 같거나 다른 제3 저장매체에 상기 이관도구를 설치하는 배포기로 구성되며, 상기 이관도구는 상기 배포기에 의해 설치된 상기 제3 저장매체에서만 실행될 수 있다.

[0018] 상기한 본 발명의 목적을 실현하기 위한 일 실시예에 따른, 디지털 포렌식 기반의 대용량 전자기록물 이관 방법은 제1 저장매체에 저장된 파일들 중 적어도 하나 이상의 파일의 속성 정보를 포함하는 이관 대상 파일 목록을 생성하는 파일 목록 생성 단계; 병렬 처리되는 입력 쓰레드, 해시 계산 쓰레드 및 출력 쓰레드 중 적어도 하나 이상을 생성하는 쓰레드 생성 단계; 상기 입력 쓰레드를 이용하여, 상기 제1 저장매체에 저장된 파일들 중 상기 이관 대상 파일 목록에 포함된 파일을 읽어 메모리에 저장하는 파일 입력 단계; 상기 해시 계산 쓰레드를 이용하여, 상기 메모리에 저장된 파일의 해시값을 계산하는 해시 계산 단계; 상기 출력 쓰레드를 이용하여, 상기 메모리에 저장된 파일을 제2 저장매체에 저장하는 파일 출력 단계; 및 상기 제2 저장매체에 저장된 파일 각각의 속성 정보 및 상기 해시값을 포함하는 수집 목록 파일을 생성하는 결과 출력 단계;를 포함한다.

[0019] 본 발명의 일 실시예에 있어서, 포맷 분석 쓰레드를 이용하여, 상기 메모리에 저장된 파일의 확장자가 파일의 형식과 일치하는지 분석하는 포맷 분석 단계;를 더 포함하고, 상기 쓰레드 생성 단계는 상기 입력 쓰레드, 상기 해시 계산 쓰레드 및 상기 출력 쓰레드와 병렬 처리되는 상기 포맷 분석 쓰레드를 더 생성하며, 상기 수집 목록 파일은 상기 포맷 분석 단계에서 분석된 결과를 더 포함할 수 있다.

[0020] 본 발명의 일 실시예에 있어서, 손상 탐지 쓰레드를 이용하여, 상기 메모리에 저장된 파일이 손상되었는지를 탐지하는 손상 탐지 단계;를 더 포함하고, 상기 쓰레드 생성 단계는 상기 입력 쓰레드, 상기 해시 계산 쓰레드 및 상기 출력 쓰레드와 병렬 처리되는 상기 손상 탐지 쓰레드를 더 생성하며, 상기 수집 목록 파일은 상기 손상 탐지 단계에서 탐지된 결과를 더 포함할 수 있다.

[0021] 본 발명의 일 실시예에 있어서, 암호파일 탐지 쓰레드를 이용하여, 상기 메모리에 저장된 파일에 암호가 설정되어 있는지를 탐지하는 암호파일 탐지 단계;를 더 포함하고, 상기 쓰레드 생성 단계는 상기 입력 쓰레드, 상기 해시 계산 쓰레드 및 상기 출력 쓰레드와 병렬 처리되는 상기 암호파일 탐지 쓰레드를 더 생성하며, 상기 수집 목록 파일은 상기 암호파일 탐지 단계에서 탐지된 결과를 더 포함할 수 있다.

[0022] 본 발명의 일 실시예에 있어서, 상기 메모리는 서로 다른 사이즈들로 사전 선언된 버퍼 메모리들을 포함하고, 상기 파일 입력 단계는 상기 사전 선언된 버퍼 메모리들 중 읽어 들일 파일의 크기에 대응되는 버퍼 메모리를 동적으로 할당받아 파일 읽기 동작을 수행할 수 있다.

[0023] 본 발명의 일 실시예에 있어서, 상기 파일 입력 단계는 상기 사전 선언된 버퍼 메모리들 중 읽어 들일 파일의 크기에 대응되는 버퍼 메모리가 없는 경우 가장 큰 사이즈의 버퍼 메모리를 복수회 이용하여 파일 읽기 동작을 수행할 수 있다.

[0024] 본 발명의 일 실시예에 있어서, 상기 제2 저장매체에 저장된 파일의 해시값은 상기 제1 저장매체에 저장된 파일의 해시값과 동일할 수 있다.

[0025] 본 발명의 일 실시예에 있어서, 상기 제2 저장매체에 저장된 파일의 생성 시간, 수정 시간 및 접근 시간은 각각 상기 제1 저장매체에 저장된 파일의 생성 시간, 수정 시간 및 접근 시간과 동일할 수 있다.

[0026] 본 발명의 일 실시예에 있어서, 상기 파일 목록 생성 단계, 상기 쓰레드 생성 단계, 상기 파일 입력 단계, 상기 해시 계산 단계, 상기 파일 출력 단계 및 상기 결과 출력 단계를 실행시키기 위한 이관도구 프로그램을 상기 제2 저장매체와 같거나 다른 제3 저장매체에 설치하는 배포 단계;를 더 포함하고, 상기 이관도구 프로그램은 상기 배포 단계에서 설치된 상기 제3 저장매체에서만 실행될 수 있다.

발명의 효과

[0027] 이와 같은 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템 및 방법에 따르면, 전자기록물의 진본성, 무결성, 신뢰성 및 이용가능성을 보장하면서 이관 속도를 향상시킬 수 있다.

[0028] 또한, 이관 결과 및 파일 분석 결과에 대한 데이터베이스를 구축하여 이관된 파일에 대한 신뢰성을 더욱 향상시킬 수 있다.

도면의 간단한 설명

[0029] 도 1은 본 발명의 일 실시예에 따른 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템을 나타내는 블록도이다.

도 2는 본 발명의 일 실시예에 따른 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템을 설명하기 위한 개념도이다.

도 3은 도 1의 이관도구를 나타내는 블록도이다.

도 4는 도 3의 파일 분석부를 나타내는 블록도이다.

도 5는 도 1의 이관도구가 복수의 쓰레드를 이용하여 파일을 이관하는 과정을 설명하기 위한 개념도이다.

도 6는 본 발명의 일 실시예에 따른 디지털 포렌식 기반의 대용량 전자기록물 이관 방법을 나타내는 순서도이다.

도 7은 도 6의 사본 저장용 저장매체로 이관하는 단계를 설명하기 위한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0030] 이하에서, 첨부한 도면들을 참조하여, 본 발명을 보다 상세하게 설명하고자 한다.

[0031] 도 1은 본 발명의 일 실시예에 따른 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템을 나타내는 블록도이다. 도 2는 본 발명의 일 실시예에 따른 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템을 설명하기 위한 개념도이다.

[0032] 본 발명에 있어서 전자기록물의 이관이란, 이관 대상 저장매체에 저장되어 있는 원본 파일을 동일성을 유지한 상태로 복사하여 사본 파일을 만들고, 이를 사본 저장용 저장매체에 저장하는 것을 의미한다.

[0033] 도 1 및 도 2를 참조하면, 본 발명의 일 실시예에 따른 디지털 포렌식 기반의 대용량 전자기록물 이관 시스템(1)은 이관도구(10) 및 배포기(20)를 포함할 수 있다.

[0034] 이관도구(10)는 제1 저장매체(30)(즉, 이관 대상 저장매체)에 저장된 원본 파일들 전부 또는 일부를 제2 저장매체(40)(즉, 사본 저장용 저장매체)로 이관할 수 있다. 이관도구(10)는 제2 저장매체(40)와 같거나 다른 제3 저장매체(미도시)에 설치된 컴퓨터 프로그램일 수 있다. 이관도구(10)는 제1 저장매체(30)가 설치되어 있는 시스템(2)(이하, 이관 대상 시스템)에 연결되어 실제 이관 기능을 수행할 수 있다.

[0035] 이관 대상 시스템(2)은 데스크탑 컴퓨터, 노트북, 태블릿, 서버 등 저장매체를 통해 파일들을 기록하고 있는 컴퓨팅 장치일 수 있다.

[0036] 제1 저장매체(30)는 이관 대상 시스템(2)에 장착되어 있는 하드 디스크 드라이브(Hard Disk Drive, HDD), 솔리드 스테이트 드라이브(Solid State Drive, SDD), 메모리 카드(예를 들어, SD카드, microSD카드 등), 플래시 메모리(Flash Memory) 등을 포함할 수 있다.

[0037] 제2 저장매체(40) 및 제3 저장매체는 USB 포트를 통해 컴퓨터에 연결될 수 있는 플래시 메모리, 외장형 HDD, 외장형 SSD 등의 이동식 저장장치를 포함할 수 있으나, 이에 한정되는 것은 아니며, 컴퓨터에 결합되어 컴퓨터 운영 시스템에 연결될 수 있는 내장형 HDD, 내장형 SSD, 메모리 카드(예를 들어, SD카드, microSD카드) 등 모든 종류의 저장매체를 포함할 수 있다.

[0038] 일 실시예에서, 이관도구(10)는 제3 저장매체에 설치된 이관 프로그램일 수 있으며, 이관 대상 시스템(2)과 USB 포트를 통해 연결될 수 있다. 이관도구(10)는 이관 대상 시스템(2)에 의해 실행되어 제1 저장매체(30)에 저장되어 있는 파일을 제2 저장매체(40)로 이관시킬 수 있다.

[0039] 한편, 이관도구(10)는 시스템에 설치되는 과정에서 발생할 수 있는 이관 대상 시스템(2)에 대한 변경을 방지할 필요가 있다. 또한, 이관도구(10)는 이관 대상 시스템(2)의 운영체제(Operating System, OS)의 종류 내지는 버전 등의 시스템 환경과 무관하게 실행될 필요가 있다. 이를 위해서, 이관도구(10)는 이관 대상 시스템(2)에 대한 별도의 인스톨(install) 과정을 거치지 않고 이관 대상 시스템(2) 상에서 실행될 수 있는 무설치 프로그램일 수 있다.

[0040] 이관도구(10)가 설치되는 제3 저장매체는 이관되는 파일이 저장되는 제2 저장매체(40)와 동일한 저장매체일 수 있다. 이와는 달리, 이관도구(10)가 설치되는 제3 저장매체는 이관되는 파일이 저장되는 제2 저장매체(40)와 다른 저장매체일 수 있다.

[0041] 일 실시예에서, 제2 저장매체(40)는 제3 저장매체와 물리적으로 동일한 저장매체일 수 있다. 이 경우, 제2 저장매체(40)는 동일한 드라이브 내에 폴더를 구분하여 이관도구(10)와 이관된 사본 파일들을 저장할 수 있다. 예를 들어, 제2 저장매체(40)는 D 드라이브를 포함하고, 이관도구(10)는 D 드라이브의 제1 하위폴더에 저장되고, 이관된 사본 파일들은 D 드라이브의 제2 하위폴더에 저장될 수 있다.

[0042] 또는, 제2 저장매체(40)는 파티션 설정 소프트웨어 등을 이용해 내부 저장공간을 나누어 2개의 드라이브를 포함할 수 있으며, 이관도구(10)와 이관된 사본 파일들을 별도의 드라이브에 저장할 수 있다. 예를 들어, 제2 저장매체(40)는 D 드라이브와 F 드라이브를 포함하고, 이관도구(10)는 D 드라이브에 저장되며, 이관된 사본 파일들은 F 드라이브에 저장될 수 있다.

[0043] 다른 실시예에서, 제2 저장매체(40)는 제3 저장매체와 물리적으로 구분되는 저장매체일 수 있다. 이 경우, 이관도구(10)는 제3 저장매체에 저장되고, 이관된 사본 파일들은 제2 저장매체(40)에 저장될 수 있다.

[0044] 배포기(20)는 제2 저장매체(40)와 같거나 다른 제3 저장매체에 이관도구(10)를 설치(S100)할 수 있다. 배포기

(20)는 허가된 사용자만이 이관도구(10)를 사용할 수 있도록 보안이 적용될 수 있다. 예를 들어, 배포기(20)는 관리자 권한을 가진 담당자만 보유 및 사용할 수 있다. 배포기(20)는 이관도구(10)를 사용할 사용자 및 이관도구(10)가 설치될 저장매체를 각각 지정하여 이관도구(10)를 배포할 수 있다. 여기서 이관도구(10)의 배포란 지정된 저장매체에 이관도구(10)를 설치하는 것을 의미한다.

[0045] 일 실시예에서, 배포기(20)는 컴퓨터일 수 있으나, 이에 한정되는 것은 아니며 저장매체를 연결하여 컴퓨터 프로그램을 실행할 수 있는 다양한 종류의 컴퓨팅 장치를 포함할 수 있다. 예를 들어, 배포기는 노트북, 태블릿, 스마트폰, PDA 등을 포함할 수 있다.

[0046] 배포기(20)는 배포된 이관도구(10)의 오용을 방지하기 위하여 이관도구(10) 사용자에 대한 정보 및 이관도구(10) 사용을 위한 인증코드를 설정할 수 있다. 이관도구(10) 사용자에 대한 정보는 사용자 이름, 소속 및 직급 등을 포함할 수 있다. 이관도구(10) 사용을 위한 인증코드는 예를 들어 패스워드일 수 있다. 또한, 배포기(20)는 배포된 이관도구(10)가 일정기간 동안만 사용될 수 있도록 사용 만료일을 지정할 수 있다.

[0047] 배포기(20)는 배포된 이관도구(10)가 복제되어 사용되는 것을 방지하기 위하여, 배포당시 특정된 저장매체에서만 실행되도록 설정할 수 있다. 이를 위하여 배포기(20)는 설치될 저장매체의 고유한 정보를 이용하여 이관도구(10)를 저장매체에 설치할 수 있다. 일 실시예에서, 저장매체의 고유한 정보는 제품 아이디(Product ID), 일련번호(Serial Number), 제조사 아이디(Vendor ID) 등을 포함할 수 있다. 따라서, 배포기(20)가 이관도구(10)를 제3 저장매체에 배포하는 경우, 이관도구(10)는 배포기(20)에 의해 설치된 제3 저장매체에서만 실행될 수 있다.

[0048] 이하에서 도 3 내지 도 7을 참조하여 이관도구(10)에 대해 자세하게 설명한다.

[0049] 도 3은 도 1의 이관도구를 나타내는 블록도이다. 도 4는 도 3의 파일 분석부를 나타내는 블록도이다. 도 5는 도 1의 이관도구가 복수의 쓰레드를 이용하여 파일을 이관하는 과정을 설명하기 위한 개념도이다. 도 6는 본 발명의 일 실시예에 따른 디지털 포렌식 기반의 대용량 전자기록물 이관 방법을 나타내는 순서도이다. 도 7은 도 6의 사본 저장용 저장매체로 이관하는 단계를 설명하기 위한 순서도이다.

[0050] 이관도구(10)는 배포기(20)를 통해 제2 저장매체(40)와 같거나 다른 제3 저장매체에 설치(S100)될 수 있다. 이관도구(10)는 파일 목록 생성부(100), 쓰레드 생성부(200), 파일 입력부(300), 해시 계산부(400), 파일 출력부(500), 파일 분석부(600), 결과 출력부(700), 제어부(800) 및 무결성 검증부(900)를 포함할 수 있다.

[0051] 파일 목록 생성부(100)는 제1 저장매체(30)에 저장된 이관 대상 원본 파일들 중 적어도 하나 이상의 파일의 속성 정보를 포함하는 이관 대상 파일 목록을 생성(S200)할 수 있다.

[0052] 파일 목록 생성부(100)는 제1 저장매체(30)의 파일시스템에 저장된 파일 노드 정보를 활용하여 제1 저장매체(30)에 저장된 파일들의 속성 정보를 획득할 수 있다. 여기서 파일의 속성 정보는 메타 데이터(Meta Data)로도 지칭되며, 파일명(File Name), 파일 용량(File Size), 수정 시간(Modification Time), 생성 시간(Creation Time), 접근 시간(Access Time), 파일경로(File Path)를 포함할 수 있다. 이관 대상 파일 목록은 파일의 속성 정보 중 적어도 하나 이상을 포함할 수 있다.

[0053] 이관도구(10)는 파일의 속성 정보를 포함하는 이관 대상 파일 목록을 활용하여 제1 저장매체(30)에 저장된 파일들 중 이관 대상 파일 목록에 포함된 파일을 제2 저장매체(40)로 이관할 수 있다(S300). 이관도구(10)는 제2 저장매체(40)로 이관된 파일에 대한 정보를 기초로 수집 목록 파일을 생성(또는 이관된 파일에 대한 정보를 기초로 수집 목록 파일 갱신)하고, 이관 과정에서 발생한 이벤트(작업 내용 및 장애 발생 내용)에 대한 로그 정보를 생성할 수 있으며, 포맷 분석부(610)의 분석 결과, 손상 탐지부(620)의 탐지 결과 및 암호파일 탐지부(630)의 탐지 결과를 포함하는 분석 결과 데이터베이스를 생성할 수 있다(S301). 이관도구(10)는 이관 대상 파일 목록에 포함된 모든 파일에 대하여 이관 작업을 완료할 때까지 단계 S300 및 단계 S301을 반복할 수 있다(S400). 일 실시예에서, 이관도구(10)는 제1 저장매체(30)에 저장된 파일들 중 이관 대상 파일 목록에 포함된 파일들을 순번에 따라 첫 번째 파일부터 순차적으로 제2 저장매체(40)로 이관할 수 있으나, 이에 한정되는 것은 아니며, 시스템 성능에 따라 적어도 하나 이상의 파일들을 동시에 처리하도록 구현될 수 있다.

[0054] 쓰레드 생성부(200)는 병렬 처리되는 입력 쓰레드(301), 해시 계산 쓰레드(401), 출력 쓰레드(501), 포맷 분석 쓰레드(611), 손상 탐지 쓰레드(621) 및 암호파일 탐지 쓰레드(631) 중 적어도 하나 이상을 생성(S310)할 수 있다.

[0055] 여기서, 쓰레드(thread)란 프로그램(또는 프로세스) 내에서 실행되는 흐름의 단위를 의미하며, 둘 이상의 쓰레드를 동시에 실행하는 방식을 멀티-쓰레드(multi-thread)라고 한다.

[0056] 파일 입력부(300)는 쓰레드 생성부(200)에서 생성된 입력 쓰레드(301)를 이용하여, 제1 저장매체(30)에 저장된 파일들 중 이관 대상 파일 목록에 포함된 파일을 읽어 메모리(50)에 저장(S320)할 수 있다. 메모리(50)는 미리 정해진 서로 다른 사이즈들로 사전 선언된 버퍼 메모리(51)들을 포함할 수 있다.

[0057] 파일 입력부(300)는 사전 선언된 버퍼 메모리(51)들 중 읽어 들일 파일의 크기에 대응되는 버퍼 메모리(51)를 동적으로 할당받아 파일을 읽을 수 있다. 예를 들어, 파일 입력부(300)는 읽어 들일 파일의 크기보다 큰 사이즈의 버퍼 메모리(51)를 동적으로 할당받아 파일을 읽을 수 있다. 파일 입력부(300)는 사전 선언된 버퍼 메모리(51)들 중 읽어 들일 파일의 크기에 대응되는 버퍼 메모리(51)가 없는 경우(즉, 사전 선언된 버퍼 메모리(51)들 중 읽어 들일 파일의 크기보다 큰 버퍼 메모리(51)가 없는 경우) 가장 큰 사이즈의 버퍼 메모리(51)를 복수회 이용하여 파일을 읽을 수 있다.

[0058] 파일 입력부(300)는, 입력 쓰레드(301)를 이용하여, 이관 대상 파일 목록에 포함된 파일의 속성 정보를 기초로 이관될 파일의 모든 데이터를 비트스트림 방식으로 읽어 버퍼 메모리(51)에 저장할 수 있으며, 이러한 버퍼 메모리(51)들이 모여 큐 공유 메모리(52)를 구성할 수 있다.

[0059] 일 실시예에서, 이관도구(10)가 제1 저장매체(30)를 포함하는 이관 대상 시스템(2)에 연결되어 이관 기능을 수행하는 경우, 버퍼 메모리(51)와 큐 공유 메모리(52)는 이관 대상 시스템(2)의 메모리(50)에 포함된 버퍼 및 큐 공유 메모리일 수 있다.

[0060] 이와는 달리, 제1 저장매체(30)가 이관 대상 시스템(2)으로부터 분리되어 이관되는 경우(예를 들어, 이관도구(10)가 설치되어 있는 이관용 컴퓨터 시스템에 이관 대상인 제1 저장매체(30)를 연결하여 이관하는 경우), 버퍼 메모리(51)와 큐 공유 메모리(52)는 이관용 컴퓨터 시스템의 메모리에 포함된 버퍼 및 큐 공유 메모리일 수 있다.

[0061] 해시 계산부(400)는, 해시 계산 쓰레드(401)를 이용하여, 메모리(50)에 저장되어 있는 파일의 해시값을 계산(S330)할 수 있다. 구체적으로 해시 계산부(400)는, 해시 계산 쓰레드(401)를 이용하여, 큐 공유 메모리(52)로부터 이관될 파일을 획득할 수 있으며, 획득한 파일을 이용하여 해시값을 계산할 수 있다.

[0062] 여기서 해시값(hash value)은 특정 파일을 고정된 길이의 데이터로 매핑하는 알고리즘을 통해 생성된 값으로, 이러한 해시값을 생성하는 알고리즘으로는 MD5, SHA-1, SHA-2 등의 해시 알고리즘(또는 해시 함수)이 사용될 수 있으나, 이에 한정되는 것은 아니다.

[0063] 해시값이 다르다면 각 해시값의 원본 파일도 서로 상이한 파일이라는 것이 해시값의 특징이므로, 이관 작업을 통해 이관된 파일의 해시값이 원본 파일의 해시값과 다르다면 진본성, 무결성 및 신뢰성이 보장되지 않는 경우에 해당한다고 판단할 수 있다.

[0064] 파일 출력부(500)는 출력 쓰레드(501)를 이용하여, 메모리(50)에 저장된 파일을 제2 저장매체(40)에 저장(S370)할 수 있다. 구체적으로 파일 출력부(500)는, 출력 쓰레드(501)를 이용하여, 큐 공유 메모리(52)로부터 이관될 파일을 획득할 수 있으며 획득한 파일을 제2 저장매체(40)에 저장할 수 있다.

[0065] 제2 저장매체(40)에 이관된 사본 파일의 해시값은 제1 저장매체(30)에 저장된 원본 파일의 해시값과 동일할 수 있다. 또한, 제2 저장매체(40)에 이관된 사본 파일의 수정 시간, 생성 시간 및 접근 시간은 제1 저장매체(30)에 저장된 원본 파일의 수정 시간, 생성 시간 및 접근 시간과 동일할 수 있다. 일 실시예에서, 이관 과정에서 제2 저장매체(40)에 이관된 사본 파일의 수정 시간, 생성 시간 및 접근 시간이 변경된 경우, 파일 출력부(500)는 이관 대상 파일 목록에 포함된 원본 파일의 수정 시간, 생성 시간 및 접근 시간을 기초로 사본 파일의 수정 시간, 생성 시간 및 접근 시간을 변경할 수 있다.

[0066] 파일 분석부(600)는 포맷 분석부(610), 손상 탐지부(620) 및 암호파일 탐지부(630)를 포함할 수 있다.

[0067] 포맷 분석부(610)는 포맷 분석 쓰레드(611)를 이용하여, 메모리(50)에 저장된 파일의 확장자가 파일의 형식과 일치하는지 분석(S340)할 수 있다. 구체적으로 포맷 분석부(610)는, 포맷 분석 쓰레드(611)를 이용하여, 큐 공유 메모리(52)로부터 이관될 파일을 획득할 수 있으며 획득한 파일을 이용하여 파일의 확장자가 파일의 형식과 일치하는지 여부를 분석할 수 있다.

[0068] 예를 들어, 포맷 분석부(610)는 파일 형식 별로 가지고 있는 고유의 파일 시그니처(File Signature) 정보를 통해 파일의 형식을 확인하고, 이를 확장자와 비교하여 파일의 확장자가 파일의 형식과 일치하는지 여부를 분석할 수 있다.

[0069] 손상 탐지부(620)는 손상 탐지 쓰레드(621)를 이용하여, 메모리(50)에 저장된 파일이 손상되었는지 여부를 탐지(S350)할 수 있다. 구체적으로 손상 탐지부(620)는, 손상 탐지 쓰레드(621)를 이용하여, 큐 공유 메모리(52)로부터 이관될 파일을 획득할 수 있으며 획득한 파일을 이용하여 파일의 손상 여부를 탐지할 수 있다.

[0070] 예를 들어, 손상 탐지부(620)는 파일 패턴 분석을 통해 손상패턴을 탐지하고, 손상패턴이 발견되는 경우 파일의 손상 여부를 확인할 수 있다.

[0071] 암호파일 탐지부(630)는 암호파일 탐지 쓰레드(631)를 이용하여, 메모리(50)에 저장된 파일에 암호가 설정되어 있는지 여부를 탐지(S360)할 수 있다. 구체적으로 암호파일 탐지부(630)는, 암호파일 탐지 쓰레드(631)를 이용하여, 큐 공유 메모리(52)로부터 이관될 파일을 획득할 수 있으며 획득한 파일을 이용하여 파일에 암호가 설정되어 있는지 여부 및/또는 디지털 저작권 관리(Digital Rights Management, DRM) 기능이 설정되어 있는지 여부를 탐지할 수 있다.

[0072] 일 실시예에서, 이관도구(10)는 파일 형식 비교를 위한 파일 형식별 고유의 파일 시그니처 정보, 손상 탐지를 위한 파일 형식별 손상패턴 및 암호파일 탐지를 위한 파일 형식별 암호화 정보를 포함하는 파일 분석 데이터베이스를 포함할 수 있으며, 포맷 분석부(610), 손상 탐지부(620) 및 암호파일 탐지부(630)는 파일 분석 데이터베이스에 기초하여 파일을 분석할 수 있다.

[0073] 예를 들어, 포맷 분석부(610)는 큐 공유 메모리(52)에 저장된 파일 및 파일 분석 데이터베이스에 저장된 파일 형식별 고유의 파일 시그니처 정보에 기초하여 파일 확장자가 파일의 형식과 일치하는지를 분석할 수 있다. 손상 탐지부(620)는 큐 공유 메모리(52)에 저장된 파일 및 파일 분석 데이터베이스에 저장된 파일 형식별 손상패턴에 기초하여 파일의 손상 여부를 탐지할 수 있다. 암호파일 탐지부(630)는 큐 공유 메모리(52)에 저장된 파일 및 파일 분석 데이터베이스에 저장된 파일 형식별 암호화 정보에 기초하여 파일에 암호가 설정되어 있는지 여부를 탐지할 수 있다.

[0074] 상기 기재된 바와 같이, 입력 쓰레드(301), 해시 계산 쓰레드(401), 출력 쓰레드(501), 포맷 분석 쓰레드(611), 손상 탐지 쓰레드(621) 및 암호파일 탐지 쓰레드(631)는 병렬 처리되어 동시에 실행될 수 있으며, 이를 통해 이관 속도를 향상시킬 수 있다.

[0075] 결과 출력부(700)는 이관 결과 보고서를 생성(S500)할 수 있다. 또한, 결과 출력부(700)는 수집 목록 파일 및 로그 정보를 생성할 수 있다.

[0076] 결과 출력부(700)는 제2 저장매체(40)에 저장된 파일 각각의 속성 정보, 해시값, 포맷 분석부(610)의 분석 결과, 손상 탐지부(620)의 탐지 결과 및 암호파일 탐지부(630)의 탐지 결과를 포함하는 수집 목록 파일을 생성할 수 있다. 일 실시예에서, 수집 목록 파일은 각각의 파일에 대한 이관 작업이 수행될 때마다 이관된 파일에 대한 정보(즉, 파일 속성 정보, 해시값, 포맷 분석부(610)의 분석 결과, 손상 탐지부(620)의 탐지 결과 및 암호파일 탐지부(630)의 탐지 결과)를 기초로 갱신될 수 있다.

[0077] 수집 목록 파일에 포함된 속성 정보는 파일명(File Name), 파일 용량(File Size), 수정 시간(Modification Time), 생성 시간(Creation Time), 접근 시간(Access Time), 파일경로(File Path) 중 적어도 하나 이상을 포함할 수 있다.

[0078] 결과 출력부(700)는 포맷 분석부(610)의 분석 결과, 손상 탐지부(620)의 탐지 결과 및 암호파일 탐지부(630)의 탐지 결과를 포함하는 분석 결과 데이터베이스를 생성할 수 있다. 일 실시예에서, 분석 결과 데이터베이스는 각각의 파일에 대한 이관 작업이 수행될 때마다 이관된 파일에 대한 분석 결과(즉, 포맷 분석부(610)의 분석 결과, 손상 탐지부(620)의 탐지 결과 및 암호파일 탐지부(630)의 탐지 결과)를 기초로 갱신될 수 있다.

[0079] 결과 출력부(700)는 이관 작업 내용 및 장애 발생 내용 등 이관 과정에서 발생된 이벤트에 대한 로그 정보를 생성할 수 있다. 일 실시예에서 로그 정보는 각각의 파일에 대한 이관 작업이 수행될 때마다 이관 과정에서 발생된 이벤트를 기초로 생성될 수 있다.

[0080] 장애 발생 내용과 관련하여 로그 정보는 파일 읽기 실패, 파일 쓰기 실패, 해시값 계산 실패 등의 정보를 포함할 수 있다. 또한, 로그 정보는 손상 탐지부(620)에 의해 손상된 파일이 탐지되는 경우 손상된 파일에 대한 탐지 정보를 포함할 수 있다. 결과 출력부(700)는 로그 정보를 기초로 손상된 파일을 필터링 하거나 별도로 선별 및 추출할 수 있다.

[0081] 결과 출력부(700)가 생성하는 로그 정보는 손상 탐지부(620)의 탐지 결과뿐만 아니라 포맷 분석부(610)의 분석 결과 및 암호파일 탐지부(630)의 탐지 결과를 포함할 수 있다. 결과 출력부(700)는 로그 정보를 기초로 포맷 형

식이 확장자와 일치하지 않는 파일, 암호가 설정된 파일 또는 DRM이 설정된 파일을 필터링 하거나 별도로 선별 및 추출할 수 있다.

[0082] 결과 출력부(700)는 이관 환경 정보, 이관 결과 정보 및 수집 목록 파일에 대한 정보를 포함하는 이관 결과 보고서를 생성할 수 있다. 이관 결과 보고서는 웹페이지 형태의 HTML(Hypertext Markup Language) 파일로 생성될 수 있다.

[0083] 이관 환경 정보는 이관에 사용된 이관도구(10) 정보, 해시값 계산에 사용된 해시 알고리즘 정보, 이관을 위해 수집된 파일의 메타 데이터 항목, 이관 대상 파일의 경로 정보 등을 포함할 수 있다.

[0084] 이관 결과 정보는 이관된 파일 건수, 이관에 소요된 시간, 이관된 파일들이 저장된 경로, 생성된 수집 목록 파일의 경로에 대한 정보를 포함할 수 있다.

[0085] 수집 목록 파일에 대한 정보는 이관 결과 생성된 수집 목록 파일에 대한 정보 및 수집 목록 파일의 해시값을 포함할 수 있다. 여기서, 수집 목록 파일의 해시값은 수집 목록 파일을 기초로 산출된 해시값을 의미한다.

[0086] 수집 목록 파일에 대한 정보는 이관된 파일 전체에 대한 해시값을 더 포함할 수 있다. 파일의 수가 많은 경우, 이관되어 보관중인 파일의 무결성을 확인하기 위해서 개별 파일들에 대하여 해시값을 계산하고, 이를 저장되어 있는 이관 당시의 해시값과 비교하는 것은 많은 시간과 노력을 필요로 한다. 이러한 경우, 이관 당시의 파일 전체에 대한 해시값을 알고 있다면 해시값을 1번만 계산해서 파일 전체가 변경되지 않았음을 확인할 수 있다. 즉, 이관되어 보관중인 파일 전체에 대하여 1번만 해시값을 계산하고, 이를 저장되어 있는 이관 당시에 계산된 파일 전체에 대한 해시값과 비교하여 쉽고 빠르게 전체 파일들에 대한 무결성을 확인할 수 있다. 이러한 측면에서, 수집 목록 파일에 대한 정보는 이관된 파일 전체에 대한 해시값을 계산하여 유지할 수 있다.

[0087] 제어부(800)는 이관도구(10) 사용자로부터 이관업무 수행과 관련된 기본 정보를 입력 받아 이관도구(10)의 기능을 제어할 수 있다.

[0088] 이관업무 수행과 관련된 기본 정보는 해시값 계산에 사용될 해시 알고리즘 종류, 수집할 메타 데이터 항목, 이관 대상 파일의 경로, 이관된 파일들이 저장될 경로, 수집 목록 파일의 생성 경로, 담당자 정보, 기록물 정보 및 이관 환경 정보를 입력받을 수 있다. 이관업무 수행과 관련된 기본 정보는 이관 종료 후 생성되는 이관 결과 보고서에 포함될 수 있다.

[0089] 담당자 정보는 이관업무와 관련된 담당자의 이름, 소속기관 및 부서에 대한 정보 등을 포함할 수 있다. 기록물 정보는 이관 대상 전자기록물 제목, 전자기록물 소속 기관 명칭, 저장매체 종류 등을 포함할 수 있다. 이관 환경 정보는 이관 작업이 수행된 장소 및 수행 장비(즉, 이관 작업이 수행된 PC에 대한 소유자 정보) 등을 포함할 수 있다.

[0090] 제어부(800)는 저장매체 단위로 이관하거나, 파일을 선택하여 이관하도록 이관도구(10)를 제어할 수 있다. 또한, 제어부(800)는 이관대상 파일 형식을 선택하여 원하는 형식의 파일들에 대해서만 이관 작업을 수행하도록 이관도구(10)를 제어할 수 있다. 예를 들어, 이관도구(10)는 사용자로부터 선택 또는 입력받은 확장자에 대응되는 형식의 파일들에 대해서만 이관 작업을 수행할 수 있다.

[0091] 무결성 검증부(900)는 이관되어 저장되어 있는 사본 파일의 무결성을 검증하기 위하여 사본 파일의 해시값을 계산하고, 계산된 해시값을 이관 당시 계산 및 저장되어 있는 해시값과 비교하여 사본 파일의 변경 여부를 확인할 수 있다. 만약 검증을 위해 계산된 해시값이 이관 당시 계산된 해시값과 상이하다면 해당 사본 파일이 변경되었다는 것을 확인할 수 있다.

[0092] 일 실시예에서, 무결성 검증부(900)는 제2 저장매체(40)에 저장되어 있는 검증 대상 사본 파일의 해시값을 계산할 수 있다. 무결성 검증부(900)는 수집 목록 파일로부터 검증 대상 사본 파일에 대응되는 해시값을 획득하고, 획득한 해시값을 검증 대상 사본 파일의 해시값과 비교할 수 있다.

[0093] 또한, 무결성 검증부(900)는 제2 저장매체(40)에 저장되어 있는 사본 파일 전체에 대하여 무결성을 검증하기 위해 사본 파일 전체에 대한 해시값을 계산할 수 있다. 무결성 검증부(900)는 이관 결과 보고서로부터 사본 파일 전체의 해시값을 획득하고, 검증을 위해 계산된 사본 파일 전체에 대한 해시값을 획득한 해시값과 비교할 수 있다.

[0094] 이상에서 살펴본 본 발명은 도면에 도시된 실시 예들을 참고로 하여 설명하였으나 이는 예시적인 것에 불과하며 당해 분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 시시예의 변형이 가능하다는 점을 이해할

것이다. 그러나, 이와 같은 변형은 본 발명의 기술적 보호 범위 내에 있다고 보아야 한다. 따라서, 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의하여 정해져야 할 것이다.

부호의 설명

[0095] 10: 이관도구 20: 배포기

30: 제1 저장매체 40: 제2 저장매체

50: 메모리 51: 버퍼 메모리

52: 큐 공유 메모리 100: 파일 목록 생성부

200: 쓰레드 생성부 300: 파일 입력부

301: 입력 쓰레드 400: 해시 계산부

401: 해시 계산 쓰레드 500: 파일 출력부

501: 출력 쓰레드 600: 파일 분석부

610: 포맷 분석부 611: 포맷 분석 쓰레드

620: 손상 탐지부 621: 손상 탐지 쓰레드

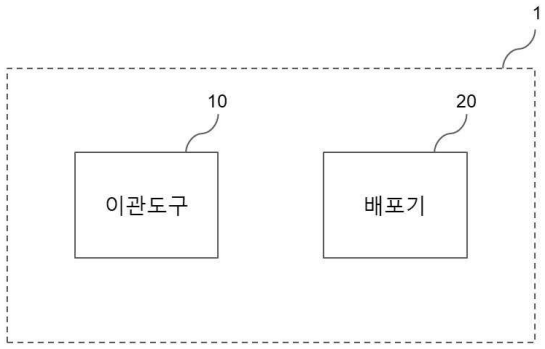
630: 암호파일 탐지부 631: 암호파일 탐지 쓰레드

700: 결과 출력부 800: 제어부

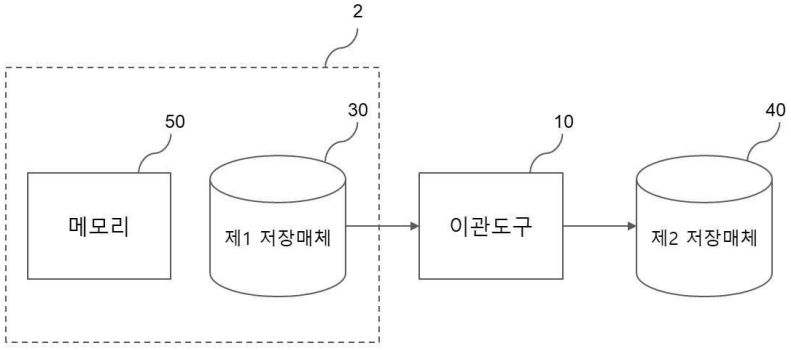
900: 무결성 검증부

도면

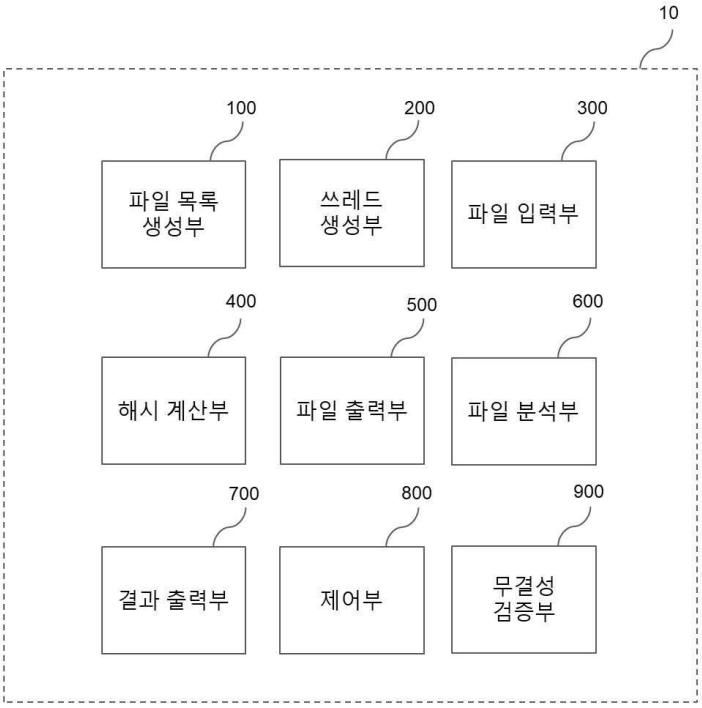
도면1



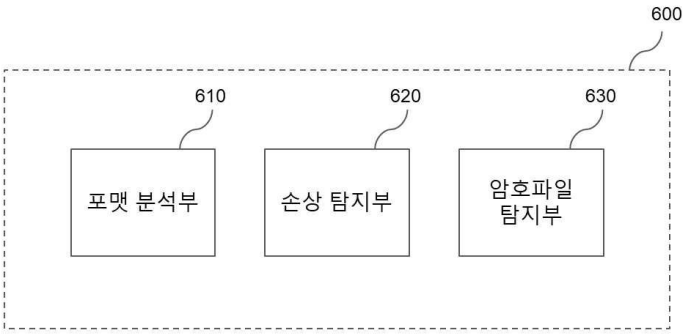
도면2



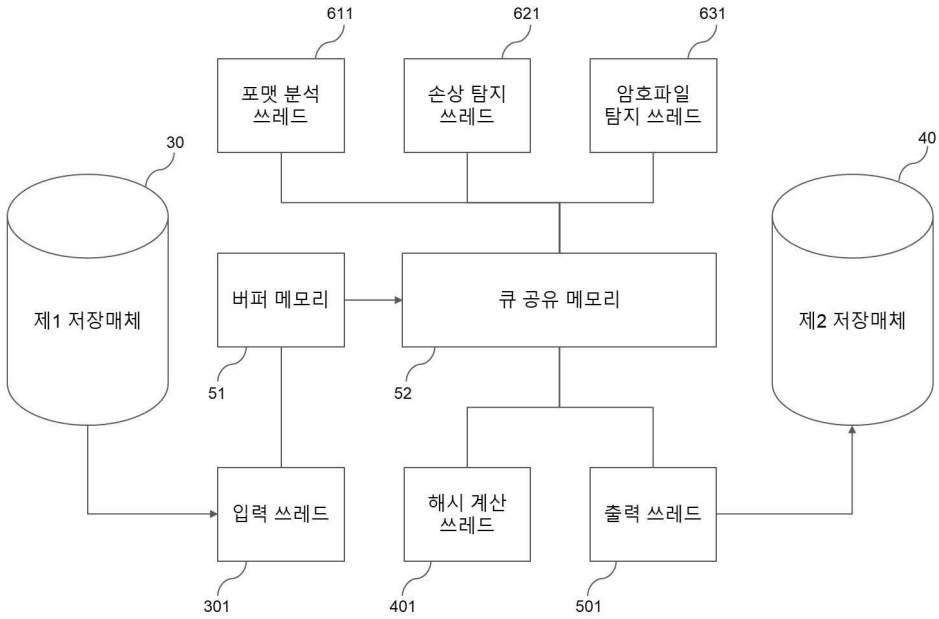
도면3


10
100
파일 목록 생성부
200
쓰레드 생성부
300
파일 입력부
400
해시 계산부
500
파일 출력부
600
파일 분석부
700
결과 출력부
800
제어부
900
무결성 검증부

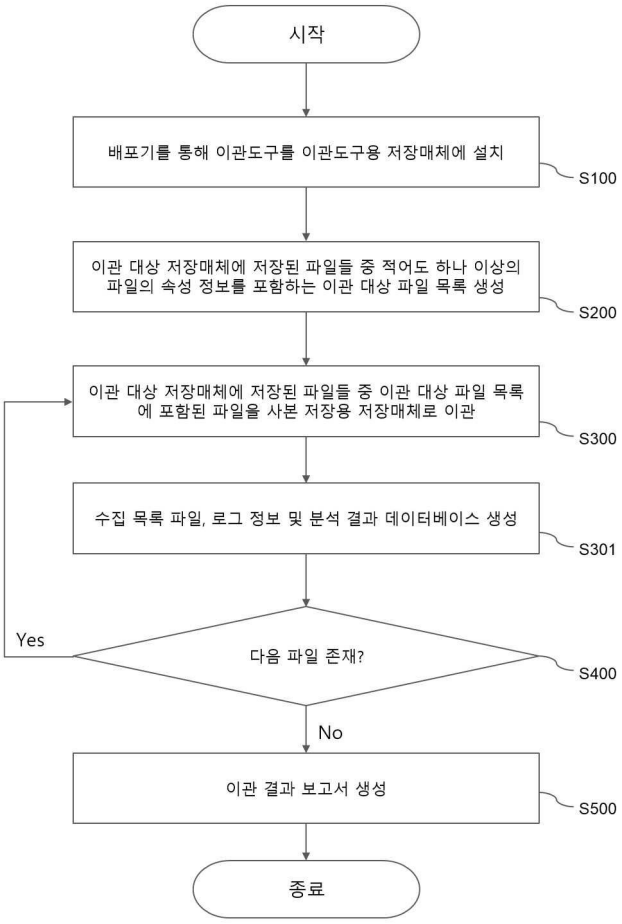
도면4


600
610
포맷 분석부
620
손상 탐지부
630
암호파일 탐지부

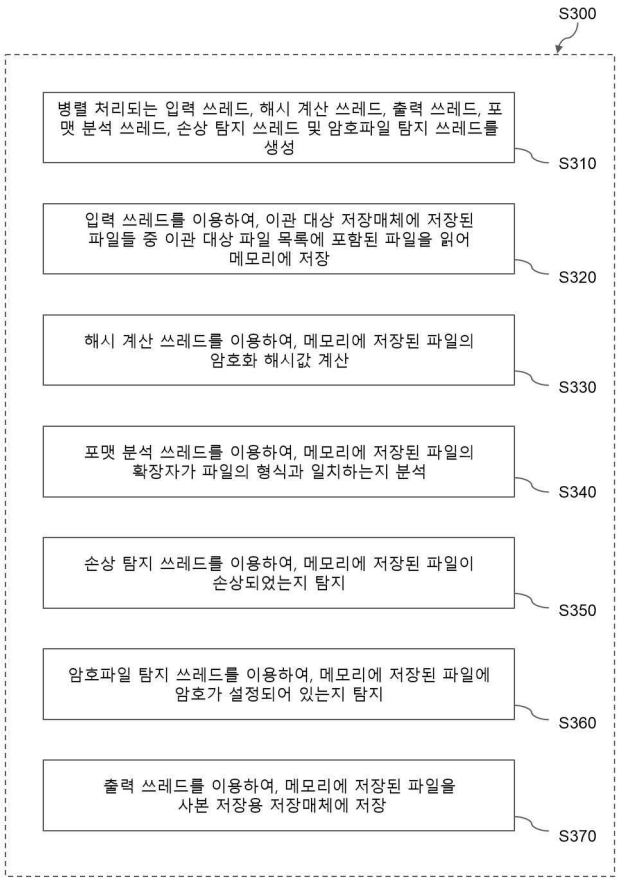
도면5


611
621
631
포맷 분석 쓰레드
손상 탐지 쓰레드
암호파일 탐지 쓰레드
30
40
제1 저장매체
버퍼 메모리
큐 공유 메모리
제2 저장매체
51
52
입력 쓰레드
해시 계산 쓰레드
출력 쓰레드
301
401
501

도면6


시작
배포기를 통해 이관도구를 이관도구용 저장매체에 설치
S100
이관 대상 저장매체에 저장된 파일들 중 적어도 하나 이상의 파일의 속성 정보를 포함하는 이관 대상 파일 목록 생성
S200
이관 대상 저장매체에 저장된 파일들 중 이관 대상 파일 목록에 포함된 파일을 사본 저장용 저장매체로 이관
S300
수집 목록 파일, 로그 정보 및 분석 결과 데이터베이스 생성
S301
다음 파일 존재?
S400
Yes
No
이관 결과 보고서 생성
S500
종료

도면7


S300
병렬 처리되는 입력 쓰레드, 해시 계산 쓰레드, 출력 쓰레드, 포맷 분석 쓰레드, 손상 탐지 쓰레드 및 암호파일 탐지 쓰레드를 생성
S310
입력 쓰레드를 이용하여, 이관 대상 저장매체에 저장된 파일들 중 이관 대상 파일 목록에 포함된 파일을 읽어 메모리에 저장
S320
해시 계산 쓰레드를 이용하여, 메모리에 저장된 파일의 암호화 해시값 계산
S330
포맷 분석 쓰레드를 이용하여, 메모리에 저장된 파일의 확장자가 파일의 형식과 일치하는지 분석
S340
손상 탐지 쓰레드를 이용하여, 메모리에 저장된 파일이 손상되었는지 탐지
S350
암호파일 탐지 쓰레드를 이용하여, 메모리에 저장된 파일에 암호가 설정되어 있는지 탐지
S360
출력 쓰레드를 이용하여, 메모리에 저장된 파일을 사본 저장용 저장매체에 저장
S370