(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0049696
(43) 공개일자 2024년04월17일

(51) 국제특허분류(Int. Cl.)
G06F 21/60 (2013.01) *G06F 16/14* (2019.01)
G06F 21/31 (2013.01) *G06F 9/455* (2018.01)
(52) CPC특허분류
G06F 21/60 (2013.01)
G06F 16/14 (2019.01)
(21) 출원번호 10-2022-0128375
(22) 출원일자 2022년10월07일
심사청구일자 2022년10월07일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이상진
서울시 종로구 사직로8길 20 파크팰리스 101동 1503호
김지언
서울특별시 성북구 고려대로24가길 17 (안암동5가, 소낭구) 507호
(뒷면에 계속)
(74) 대리인
특허법인위솔

전체 청구항 수 : 총 11 항

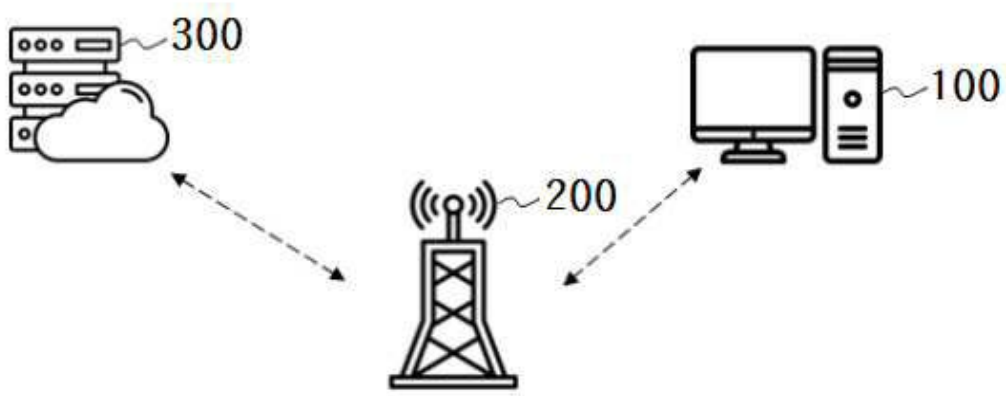
(54) 발명의 명칭 **클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법 및 이를 위한 장치**

(57) 요 약

본 발명의 일 실시 예에 따른 프로세서 및 메모리를 포함하는 장치가 클라우드(Cloud) 기반 스토리지(Storage)에 대한 디지털포렌식 데이터를 수집하는 방법은 (a) 상기 클라우드 기반 스토리지에 접속하여 로그인하는 단계, (b) 상기 로그인하여 수신한 응답으로부터 API(Application Programming Interface) 호출을 위한 공통인증정보

(뒷면에 계속)

대 표 도 - 도2



를 추출하는 단계, (c) 상기 추출한 공통인증정보와 함께 제1 API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일에 대한 목록 및 상기 목록이 포함하는 파일에 대한 메타데이터(Metadata)를 탐색하는 단계, (d) 상기 추출한 공통인증정보와 함께 제2 API 호출을 통해 상기 탐색한 목록 및 메타데이터에 대하여 수집을 위한 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하여 검색하는 단계 및 (e) 상기 추출한 공통인증정보와 함께 제3 API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일 중, 상기 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일을 선별하여 수집을 시도하는 단계를 포함한다.

(52) CPC특허분류
G06F 21/31 (2013.01)
G06F 9/45558 (2013.01)
G06F 2009/45587 (2019.08)

(72) 발명자
박정흠
서울시 마포구 마포대로 195 408동 2205호
양지혁
경기도 고양시 일산동구 경의로 47 (백석동) 1차 A동 811호
정병찬
서울특별시 동대문구 왕산로32길 47 (용두동) 라루체3, 405호
윤우성
서울특별시 강동구 천호대로 1231, 101동 1104호 (길동, 현대아파트)
방제완
서울특별시 서대문구 독립문로12나길 20 (천연동, 신세계빌라) 301호

이 발명을 지원한 국가연구개발사업

과제고유번호	9991007791
과제번호	210121M07
부처명	다부처
과제관리(전문)기관명	(재단)과학치안진흥센터
연구사업명	치안현장맞춤형연구개발(폴리스랩2.0)(R&D)(경찰청,과기정통부)
연구과제명	안티-포렌식 기술 대응을 위한 데이터 획득 및 분석 기술 연구
기 여 율	1/1
과제수행기관명	고려대학교
연구기간	2021.07.01 ~ 2024.12.31

명 세 서

청구범위

청구항 1

프로세서 및 메모리를 포함하는 장치가 클라우드(Cloud) 기반 스토리지(Storage)에 대한 디지털포렌식 데이터를 수집하는 방법에 있어서,

(a) 상기 클라우드 기반 스토리지에 접속하여 로그인하는 단계;

(b) 상기 로그인하여 수신한 응답으로부터 API(Application Programming Interface) 호출을 위한 공통인증정보를 추출하는 단계;

(c) 상기 추출한 공통인증정보와 함께 제1 API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일에 대한 파일 목록 및 상기 목록이 포함하는 파일에 대한 메타데이터(Metadata)를 탐색하는 단계;

(d) 상기 추출한 공통인증정보와 함께 제2 API 호출을 통해 상기 탐색한 목록 및 메타데이터에 대하여 수집을 위한 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하여 검색하는 단계; 및

(e) 상기 추출한 공통인증정보와 함께 제3 API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일 중, 상기 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일을 선별하여 수집하는 단계;

를 포함하는 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법.

청구항 2

제1항에 있어서,

상기 (a) 단계에서의 로그인은,

상기 클라우드 기반 스토리지의 사용자 아이디, 사용자 비밀번호, 사용자 인증 토큰 및 사용자 쿠키값 중 어느 하나 이상을 포함하는 사용자 크리덴셜(Credential)을 통해 이루어지는,

클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법.

청구항 3

제1항에 있어서,

상기 (b) 단계에서의 공통인증정보는,

상기 클라우드 기반 스토리지의 사용자 인증 토큰 및 사용자 쿠기값 중 어느 하나 이상인,

클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법.

청구항 4

제1항에 있어서,

상기 (a) 단계 및 (b) 단계 사이에,

(a′) 상기 로그인한 클라우드 기반 스토리지가 2차 인증이 필요한지 판단하는 단계; 및

(a″) 상기 판단 결과 2차 인증이 필요하다면, 상기 클라우드 기반 스토리지로부터 인증 메시지 및 인증 코드 중 어느 하나 이상을 수신하여 2차 인증을 수행하는 단계;

를 더 포함하는 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법.

청구항 5

제1항에 있어서,

상기 (c) 단계 및 (d) 단계 사이에,

(c′) 상기 탐색한 목록 및 메타데이터에 대하여 수집을 위한 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하여 검색하기 위해 추가인증정보가 필요한지 판단하는 단계; 및

(c″) 상기 판단 결과 추가인증정보가 필요하다면, 상기 클라우드 기반 스토리지에 추가인증정보를 호출하여 확보하는 단계;

를 더 포함하는 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법.

청구항 6

제5항에 있어서,

상기 (c″) 단계 이후에,

(c″′) 상기 확보한 추가인증정보와 함께 제K(여기서 K는 4 이상의 자연수) API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일에 대한 목록′ 및 상기 목록′이 포함하는 파일에 대한 메타데이터′를 재탐색하는 단계;

를 더 포함하며,

이 경우 상기 (d) 단계에서의 목록은 상기 목록′으로 대체되며,

상기 (d) 단계 및 (e) 단계에서의 메타데이터는 상기 메타데이터′로, 공통인증정보는 상기 추가인증정보로 대체되는,

클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법.

청구항 7

제1항에 있어서,

상기 (e) 단계 이후에,

(f) 상기 클라우드 기반 스토리지로부터 상기 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일이 수집되었는지 판단하는 단계;

(g) 상기 판단 결과 수집되지 않았다면, 상기 제3 API 호출에 대하여 수신한 응답으로부터 제N(여기서 N은 4 이상의 자연수) API를 추출하는 단계; 및

(h) 상기 추출한 공통인증정보와 함께 제N API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일 중, 상기 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일을 선별하여 수집을 시도하는 단계;

를 더 포함하는 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법.

청구항 8

제7항에 있어서,

상기 (h) 단계 이후에,

(i) 상기 (f) 단계로 회귀하는 단계;

를 더 포함하며,

이 경우 상기 (g) 단계에서의 제N API는 제N+1 API로 대체되는,

클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법.

청구항 9

제1항에 있어서,

상기 (c) 단계에서의 메타데이터는,

상기 클라우드 기반 스토리지에 저장된 파일의 파일명, 파일 크기, 파일 업로드 시간, 파일 수정 시간, 파일 삭제 시간, 파일을 공유 받은 자, 파일 작성자, 파일 히스토리, 썸네일, OCR, 조회수 및 조회자 중 하나 이상을 포함하는,

클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법.

청구항 10

하나 이상의 프로세서;

네트워크 인터페이스;

상기 프로세서에 의해 수행되는 컴퓨터 프로그램을 로드(Load)하는 메모리; 및

대용량 네트워크 데이터 및 상기 컴퓨터 프로그램을 저장하는 스토리지를 포함하되,

상기 컴퓨터 프로그램은 상기 하나 이상의 프로세서에 의해,

(A) 클라우드 기반 스토리지에 접속하여 로그인하는 오퍼레이션;

(B) 상기 로그인하여 수신한 응답으로부터 API(Application Programming Interface) 호출을 위한 공통인증정보를 추출하는 오퍼레이션;

(C) 상기 추출한 공통인증정보와 함께 제1 API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일에 대한 목록 및 상기 목록이 포함하는 파일에 대한 메타데이터(Metadata)를 탐색하는 오퍼레이션;

(D) 상기 추출한 공통인증정보와 함께 제2 API 호출을 통해 상기 탐색한 목록 및 메타데이터에 대하여 수집을 위한 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하여 검색하는 오퍼레이션; 및

(E) 상기 추출한 공통인증정보와 함께 제3 API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일 중, 상기 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일을 선별하여 수집을 시도하는 오퍼레이션;

을 실행하는 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 장치.

청구항 11

컴퓨팅 장치와 결합하여,

(AA) 클라우드 기반 스토리지에 접속하여 로그인하는 단계;

(BB) 상기 로그인하여 수신한 응답으로부터 API(Application Programming Interface) 호출을 위한 공통인증정보를 추출하는 단계;

(CC) 상기 추출한 공통인증정보와 함께 제1 API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일에 대한 목록 및 상기 목록이 포함하는 파일에 대한 메타데이터(Metadata)를 탐색하는 단계;

(DD) 상기 추출한 공통인증정보와 함께 제2 API 호출을 통해 상기 탐색한 목록 및 메타데이터에 대하여 수집을 위한 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하여 검색하는 단계; 및

(EE) 상기 추출한 공통인증정보와 함께 제3 API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일 중, 상기 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일을 선별하여 수집을 시도하는 단계;

를 실행하는 컴퓨터로 판독 가능한 매체에 저장된 컴퓨터 프로그램.

발명의 설명

기 술 분 야

[0001] 본 발명은 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법 및 이를 위한 장치에 관한 것이다. 보다 자세하게는 클라우드 기반 스토리지를 대상으로 디지털포렌식 활동의 효율성 향상과 피압수자의 프라이버시 강화를 도모할 수 있는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 인터넷 기술의 발달과 모바일 기기의 증가로 인해 일상 생활에서 기존과 같은 로컬 저장소가 아닌 클라우드 스토리지에 많은 양의 데이터가 저장되고 있으며, 클라우드 컴퓨팅을 통해 클라우드 스토리지에 저장된 파일을 언제 어디서든 제약 없이 접근하여 확인하거나 관리할 수 있다는 장점이 있다.

[0003] 한편, 최근의 클라우드 스토리지 서비스는 사용자 유치를 위해 서비스 제공자가 다양한 부가 기능을 함께 제공하고 있는바, 파일 공유, 공동 편집, 파일 히스토리, OCR(Optical Character Recognition) 기능 등이 대표적이며, 이러한 기능들은 클라우드 스토리지 서비스 사용자의 급격한 증가를 가져왔고, 이들 사용자들 중 일부는 범죄와 관련된 데이터를 클라우드 스토리지에 저장하기도 한다.

[0004] 이러한 범죄 관련 데이터의 수집은 디지털포렌식 활동을 통해 이루어지며, 디지털포렌식이란 디지털 증거물을 분석하여 수사에 활용하고, 디지털 증거물의 증거 능력을 향상시키기 위한 과학 수사 기법을 의미하는바, 종래에는 클라우드 스토리지에 저장된 데이터를 수집하기 위해 피압수자의 계정 정보를 확보하여 저장된 데이터를 모두 수집하고 분석하는 원시적인 방법을 취해왔다.

[0005] 그러나 클라우드 스토리지에 저장된 데이터가 많아지면서 이들 데이터를 수집하는데 소요되는 시간이 증가하며, 수집한 데이터를 저장할 저장 매체까지 따로 필요한바, 이는 디지털포렌식 활동에 필요한 비용과 자원이 증가한다는 문제점을 야기한다. 또한, 클라우드 스토리지에 저장된 모든 데이터가 범죄와 관련된 데이터가 아님에도 불구하고 일률적으로 수집의 대상이 되었던바, 피압수자의 프라이버시 침해의 문제까지 존재하였다.

[0006] 따라서 이상 설명한 디지털포렌식 활동의 효율성과 피압수자의 프라이버시 에 관한 문제점들을 해결함과 동시에 최근의 클라우드 스토리지 서비스에 적합하게 적용될 수 있는 새롭고 진보적인 기술의 개발이 요구된다. 본 발명은 이에 관한 것이다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 대한민국 공개특허공보 제 10-2013-0067607호(2013.06.25)

발명의 내용

해결하려는 과제

[0008] 본 발명이 해결하고자 하는 기술적 과제는 디지털포렌식 활동에 필요한 비용과 자원을 절감함으로써 효율성을 향상시킬 수 있는 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법 및 이를 위한 장치를 제공하는 것이다.

[0009] 본 발명이 해결하고자 하는 또 다른 기술적 과제는 클라우드 스토리지에 저장된 데이터 중, 범죄와 관련된 데이터만 선별적으로 수집함으로써 피압수자의 프라이버시를 강화할 수 있는 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법 및 이를 위한 장치를 제공하는 것이다.

[0010] 본 발명의 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0011] 상기 기술적 과제를 달성하기 위한 본 발명의 일 실시 예에 따른 프로세서 및 메모리를 포함하는 장치가 클라우드(Cloud) 기반 스토리지(Storage)에 대한 디지털포렌식 데이터를 수집하는 방법은 (a) 상기 클라우드 기반 스토리지에 접속하여 로그인하는 단계, (b) 상기 로그인하여 수신한 응답으로부터 API(Application Programming Interface) 호출을 위한 공통인증정보를 추출하는 단계, (c) 상기 추출한 공통인증정보와 함께 제1 API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일에 대한 목록 및 상기 목록이 포함하는 파일에 대한 메타데이터(Metadata)를 탐색하는 단계, (d) 상기 추출한 공통인증정보와 함께 제2 API 호출을 통해 상기 탐색한 목록 및 메타데이터에 대하여 수집을 위한 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하여 검색하는 단계 및 (e) 상기 추출한 공통인증정보와 함께 제3 API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일 중, 상기 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일을 선별하여 수집을 시도하는 단계를 포함한다.

[0012] 일 실시 예에 따르면, 상기 (a) 단계에서의 로그인은, 상기 클라우드 기반 스토리지의 사용자 아이디, 사용자 비밀번호, 사용자 인증 토큰 및 사용자 쿠키값 중 어느 하나 이상을 포함하는 사용자 크리덴셜(Credential)을 통해 이루어질 수 있다.

[0013] 일 실시 예에 따르면, 상기 (b) 단계에서의 공통인증정보는, 상기 클라우드 기반 스토리지의 사용자 인증 토큰 및 사용자 쿠기값 중 어느 하나 이상일 수 있다.

[0014] 일 실시 예에 따르면, 상기 (a) 단계 및 (b) 단계 사이에, (a′) 상기 로그인한 클라우드 기반 스토리지가 2차 인증이 필요한지 판단하는 단계 및 (a″) 상기 판단 결과 2차 인증이 필요하다면, 상기 클라우드 기반 스토리지로부터 인증 메시지 및 인증 코드 중 어느 하나 이상을 수신하여 2차 인증을 수행하는 단계를 더 포함할 수 있다.

[0015] 일 실시 예에 따르면, 상기 (c) 단계 및 (d) 단계 사이에, (c′) 상기 탐색한 목록 및 메타데이터에 대하여 수집을 위한 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하여 검색하기 위해 추가인증정보가 필요한지 판단하는 단계 및 (c″) 상기 판단 결과 추가인증정보가 필요하다면, 상기 클라우드 기반 스토리지에 추가인증정보를 호출하여 확보하는 단계를 더 포함할 수 있다.

[0016] 일 실시 예에 따르면, 상기 (c″) 단계 이후에, (c″ ′) 상기 확보한 추가인증정보와 함께 제K(여기서 K는 4 이상의 자연수) API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일에 대한 목록′ 및 상기 목록′ 이 포함하는 파일에 대한 메타데이터′ 를 재탐색하는 단계를 더 포함하며, 이 경우 상기 (d) 단계에서의 목록은 상기 목록′ 으로 대체되며, 상기 (d) 단계 및 (e) 단계에서의 메타데이터는 상기 메타데이터′ 로, 공통인증정보는 상기 추가인증정보로 대체될 수 있다.

[0017] 일 실시 예에 따르면, 상기 (e) 단계 이후에, (f) 상기 클라우드 기반 스토리지로부터 상기 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일이 수집되었는지 판단하는 단계, (g) 상기 판단 결과 수집되지 않았다면, 상기 제3 API 호출에 대하여 수신한 응답으로부터 제N(여기서 N은 4 이상의 자연수) API를 추출하는 단계 및 (h) 상기 추출한 공통인증정보와 함께 제N API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일 중, 상기 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일을 선별하여 수집을 시도하는 단계를 더 포함할 수 있다.

[0018] 일 실시 예에 따르면, 상기 (h) 단계 이후에, (i) 상기 (f) 단계로 회귀하는 단계를 더 포함하며, 이 경우 상기 (g) 단계에서의 제N API는 제N+1 API로 대체될 수 있다.

[0019] 일 실시 예에 따르면, 상기 (c) 단계에서의 메타데이터는, 상기 클라우드 기반 스토리지에 저장된 파일의 파일명, 파일 크기, 파일 업로드 시간, 파일 수정 시간, 파일 삭제 시간, 파일을 공유 받은 자, 작성자, 파일 히스토리, 썸네일, OCR, 조회수 및 조회자 중 하나 이상을 포함할 수 있다.

[0020] 상기 기술적 과제를 달성하기 위한 본 발명의 또 다른 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 장치는 하나 이상의 프로세서, 네트워크 인터페이스, 상기 프로세서에 의해 수행되는 컴퓨터 프로그램을 로드(Load)하는 메모리 및 대용량 네트워크 데이터 및 상기 컴퓨터 프로그램을 저장하는 스토리지를 포함하되, 상기 컴퓨터 프로그램은 상기 하나 이상의 프로세서에 의해, (A) 클라우드 기반 스토리지에 접속하여 로그인하는 오퍼레이션, (B) 상기 로그인하여 수신한 응답으로부터 API(Application Programming Interface) 호출을 위한 공통인증정보를 추출하는 오퍼레이션, (C) 상기 추출한 공통인증정보와 함께 제1 API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일에 대한 목록 및 상기 목록이 포함하는 파일에 대한 메타데이터(Metadata)를 탐색하는 오퍼레이션, (D) 상기 추출한 공통인증정보와 함께 제2 API 호출을 통해 상기 탐색한 목록 및 메타데이터에 대하여 수집을 위한 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하여 검색하는 오퍼레이션 및 (E) 상기 추출한 공통인증정보와 함께 제3 API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일 중, 상기 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일을 선별하여 수집을 시도하는 오퍼레이션을 실행한다.

[0021] 상기 기술적 과제를 달성하기 위한 본 발명의 또 다른 실시 예에 따른 매체에 저장된 컴퓨터 프로그램은 컴퓨팅 장치와 결합하여, (AA) 클라우드 기반 스토리지에 접속하여 로그인하는 단계, (BB) 상기 로그인하여 수신한 응답으로부터 API(Application Programming Interface) 호출을 위한 공통인증정보를 추출하는 단계, (CC) 상기 추출한 공통인증정보와 함께 제1 API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일에 대한 목록 및 상기 목록이 포함하는 파일에 대한 메타데이터(Metadata)를 탐색하는 단계, (DD) 상기 추출한 공통인증정보와 함께 제2 API 호출을 통해 상기 탐색한 목록 및 메타데이터에 대하여 수집을 위한 기간, 키워드 및 썸네일 중

어느 하나 이상을 적용하여 검색하는 단계 및 (EE) 상기 추출한 공통인증정보와 함께 제3 API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일 중, 상기 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일을 선별하여 수집을 시도하는 단계를 실행한다.

발명의 효과

[0022] 상기와 같은 본 발명에 따르면, 클라우드 기반 스토리지에 저장된 모든 파일에 대하여 무분별한 디지털포렌식 활동을 수행하는 것이 아니라, 디지털포렌식 활동을 통해 수집하고자 하는 데이터를 선별하기 위한 검색 조건을 적용한 검색 결과에 포함되는 메타데이터 그리고 이에 해당하는 데이터만을 선별하여 수집하기 때문에 클라우드 기반 스토리지에 저장된 파일 전부에 대한 디지털포렌식 활동이 필요하지 않게 되어 비용과 자원을 절감함으로써 디지털포렌식 활동의 효율성을 향상시킬 수 있다는 효과가 있다.

[0023] 또한, 디지털포렌식 활동을 통해 수집하고자 하는 데이터를 선별하기 위한 검색 조건을 적용한 검색 결과에 포함되는 메타데이터 그리고 이에 해당하는 데이터만을 선별하여 수집하기에 클라우드 기반 스토리지에 저장된 모든 데이터를 일률적으로 수집하지 않아도 되는바, 피압수자의 프라이버시를 강화할 수 있다는 효과가 있다.

[0024] 또한, 클라우드 기반 스토리지에 저장된 파일 중, 잠겨 있는 파일이 존재하더라도 이에 대한 잠김을 풀 수 있는 추가인증정보를 획득하여 잠김을 푼 후, 잠김이 풀어져 있는 상태의 파일을 포함하는 새로운 목록 및 해당 새로운 목록이 포함하는 파일에 대한 메타데이터를 재탐색하기 때문에 클라우드 기반 스토리지에 저장되어 있는 데이터의 누락 없이 디지털포렌식 활동의 정확도를 향상시킬 수 있다는 효과가 있다.

[0025] 또한, 클라우드 기반 스토리지에 저장된 파일 중, 디지털포렌식 활동을 통해 수집하고자 하는 데이터를 선별하기 위한 검색 조건을 적용한 검색 결과에 포함되는 메타데이터 그리고 이에 해당하는 데이터 중 일부라도 수집되지 않는다면, 수집을 위한 API를 재호출하여 지속적으로 수집을 시도할 수 있는바, 수집이 필요한 데이터임에도 불구하고 수집하지 못하게 되는 상황을 방지할 수 있음으로써 디지털포렌식 활동의 정확도를 향상시킬 수 있다는 효과가 있다.

[0026] 본 발명의 효과들은 이상에서 언급한 효과들로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해 될 수 있을 것이다.

도면의 간단한 설명

[0027] 도 1은 본 발명의 제1 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 장치가 포함하는 전체 구성을 예시적으로 도시한 도면이다.

도 2는 본 발명의 제2 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법이 이루어지는 환경을 도시한 도면이다.

도 3은 본 발명의 제2 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법의 대표적인 단계를 나타낸 순서도이다.

도 4는 본 발명의 제2 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법에 있어서, S350 단계가 포함하는 세부적인 단계를 나타낸 순서도이다.

도 5는 본 발명의 제3 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법의 대표적인 단계를 나타낸 순서도이다.

도 6은 본 발명의 제4 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법의 대표적인 단계를 나타낸 순서도이다.

도 7은 본 발명의 제5 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법의 대표적인 단계를 나타낸 순서도이다.

도 8은 본 발명의 제1 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 장치를 도 1의 경우와 상이하게 기능적인 구성을 포함하는 형태로 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0028] 본 발명의 목적과 기술적 구성 및 그에 따른 작용 효과에 관한 자세한 사항은 본 발명의 명세서에 첨부된 도면에 의거한 이하의 상세한 설명에 의해 보다 명확하게 이해될 것이다. 첨부된 도면을 참조하여 본 발명에 따른

실시 예를 상세하게 설명한다.

[0029] 본 명세서에서 개시되는 실시 예들은 본 발명의 범위를 한정하는 것으로 해석되거나 이용되지 않아야 할 것이다. 이 분야의 통상의 기술자에게 본 명세서의 실시 예를 포함한 설명은 다양한 응용을 갖는다는 것이 당연하다. 따라서, 본 발명의 상세한 설명에 기재된 임의의 실시 예들은 본 발명을 보다 잘 설명하기 위한 예시적인 것이며 본 발명의 범위가 실시 예들로 한정되는 것을 의도하지 않는다.

[0030] 도면에 표시되고 아래에 설명되는 기능 블록들은 가능한 구현의 예들일 뿐이다. 다른 구현들에서는 상세한 설명의 사상 및 범위를 벗어나지 않는 범위에서 다른 기능 블록들이 사용될 수 있다. 또한, 본 발명의 하나 이상의 기능 블록이 개별 블록들로 표시되지만, 본 발명의 기능 블록들 중 하나 이상은 동일 기능을 실행하는 다양한 하드웨어 및 소프트웨어 구성들의 조합일 수 있다.

[0031] 또한, 어떤 구성요소들을 포함한다는 표현은 "개방형"의 표현으로서 해당 구성요소들이 존재하는 것을 단순히 지칭할 뿐이며, 추가적인 구성요소들을 배제하는 것으로 이해되어서는 안 된다.

[0032] 나아가 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급될 때에는, 그 다른 구성요소에 직접적으로 연결 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 한다.

[0033] 이하에서는 도면들을 참조하여 본 발명의 세부적인 실시 예들에 대해 살펴보도록 한다.

[0034] 도 1은 본 발명의 제1 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 장치(100)가 포함하는 전체 구성을 예시적으로 도시한 도면이다.

[0035] 그러나 이는 본 발명의 목적을 달성하기 위한 바람직한 실시 예일 뿐이며, 필요에 따라 일부 구성이 추가되거나 삭제될 수 있고, 어느 한 구성이 수행하는 역할을 다른 구성이 함께 수행할 수도 있음은 물론이다.

[0036] 본 발명의 제1 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 장치(100)는 프로세서(10), 네트워크 인터페이스(20), 메모리(30), 스토리지(40) 및 이들을 연결하는 데이터 버스(50)를 포함할 수 있으며, 기타 본 발명의 목적을 달성함에 있어 요구되는 부가적인 구성들을 더 포함할 수 있음은 물론이라 할 것이다.

[0037] 프로세서(10)는 각 구성의 전반적인 동작을 제어한다. 프로세서(10)는 CPU(Central Processing Unit), MPU(Micro Processer Unit), MCU(Micro Controller Unit) 또는 본 발명이 속하는 기술 분야에서 널리 알려져 있는 형태의 프로세서 중 어느 하나일 수 있다. 아울러, 프로세서(10)는 본 발명의 제2 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법을 수행하기 위한 적어도 하나의 애플리케이션 또는 프로그램에 대한 연산을 수행할 수 있다.

[0038] 네트워크 인터페이스(20)는 본 발명의 제1 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 장치(100)의 유무선 인터넷 통신을 지원하며, 그 밖의 공지의 통신 방식을 지원할 수도 있다. 따라서 네트워크 인터페이스(20)는 그에 따른 통신 모듈을 포함하여 구성될 수 있다.

[0039] 메모리(30)는 각종 정보, 명령 및/또는 정보를 저장하며, 본 발명의 제2 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법을 수행하기 위해 스토리지(40)로부터 하나 이상의 컴퓨터 프로그램(41)을 로드할 수 있다. 도 1에서는 메모리(30)의 하나로 RAM을 도시하였으나 이와 더불어 다양한 저장 매체를 메모리(30)로 이용할 수 있음은 물론이다.

[0040] 스토리지(40)는 하나 이상의 컴퓨터 프로그램(41) 및 대용량 네트워크 정보(42)를 비임시적으로 저장할 수 있다. 이러한 스토리지(40)는 ROM(Read Only Memory), EPROM(Erasable Programmable ROM), EEPROM(Electrically Erasable Programmable ROM), 플래시 메모리 등과 같은 비휘발성 메모리, 하드 디스크, 착탈형 디스크, 또는 본 발명이 속하는 기술 분야에서 널리 알려져 있는 임의의 형태의 컴퓨터로 읽을 수 있는 기록 매체 중 어느 하나일 수 있다.

[0041] 컴퓨터 프로그램(41)은 메모리(30)에 로드되어, 하나 이상의 프로세서(10)에 의해, (A) 상기 클라우드 기반 스토리지에 접속하여 로그인하는 오퍼레이션, (B) 상기 로그인하여 수신한 응답으로부터 API(Application Programming Interface) 호출을 위한 공통인증정보를 추출하는 오퍼레이션, (C) 상기 추출한 공통인증정보와 함께 제1 API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일에 대한 목록 및 상기 목록이 포함하는 파일에 대한 메타데이터(Metadata)를 탐색하는 오퍼레이션, (D) 상기 추출한 공통인증정보와 함께 제2 API 호출을

통해 상기 탐색한 목록 및 메타데이터에 대하여 수집을 위한 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하여 검색하는 오퍼레이션 및 (E) 상기 추출한 공통인증정보와 함께 제3 API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일 중, 상기 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일을 선별하여 수집을 시도하는 오퍼레이션을 실행할 수 있다.

[0042] 이상 간단하게 언급한 컴퓨터 프로그램(41)이 수행하는 오퍼레이션은 컴퓨터 프로그램(41)의 일 기능으로 볼 수 있으며, 보다 자세한 설명은 본 발명의 제2 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법에 대한 설명에서 후술하도록 한다.

[0043] 데이터 버스(50)는 이상 설명한 프로세서(10), 네트워크 인터페이스(20), 메모리(30) 및 스토리지(40) 사이의 명령 및/또는 정보의 이동 경로가 된다.

[0044] 이상 설명한 본 발명의 제1 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 장치(100)는 독립된 디바이스의 형태, 예를 들어 전자 기기나 서버(클라우드 포함)의 형태일 수 있으며, 후자의 경우 전용 어플리케이션의 형태로 범죄 수사를 담당하는 수사관의 전자 기기 등에 설치될 수 있을 것이다.

[0045] 한편, 여기서 전자 기기는 스마트폰, 태블릿 PC, 노트북 PC, PDA, PMP 등과 같이 휴대가 용이한 포터블 기기 뿐만 아니라 한 장소에 고정 설치되어 사용하는 데스크톱 PC 등이라도 무방하며, 데이터의 수집 대상이 클라우드 기반 스토리지이기 때문에 네트워크 기능만 보유하고 있다면 전자 기기는 어떠한 것이라도 무방하다 할 것이다.

[0046] 이하, 본 발명의 제1 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 장치(100)가 독립된 디바이스 형태임을 전제로 본 발명의 제2 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법에 대하여 도 2 내지 도 7을 참조하여 설명하도록 한다.

[0047] 도 2는 본 발명의 제2 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법이 이루어지는 환경을 도시한 도면이며, 도3은 본 발명의 제2 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법의 대표적인 단계를 나타낸 순서도이다.

[0048] 그러나 이는 본 발명의 목적을 달성함에 있어서 바람직한 실시 예일 뿐이며, 필요에 따라 일부 단계가 추가 또는 삭제될 수 있음은 물론이고, 어느 한 단계가 다른 단계에 포함되어 수행될 수도 있다.

[0049] 한편, 각 단계는 본 발명의 제1 실시 예에 따른 클라우드 기반 스토리지(300)에 대한 디지털포렌식 데이터를 수집하는 장치(100)를 통해 이루어지는 것을 전제로 하며, 설명의 편의를 위해 "장치(100)"로 명명하도록 하며, "파일"은 클라우드 기반 스토리지(300)에 저장된 데이터 또는 컨텐츠를 의미하는 단어인바, "데이터", "컨텐츠"와 혼용되어 같은 의미로써 사용될 수 있음을 미리 밝혀두는 바이다.

[0050] 우선, 장치(100)가 클라우드 기반 스토리지(300)에 접속하여 로그인한다(S310).

[0051] 여기서의 접속은 도 2에 도시된 바와같이 장치(100)가 네트워크(200)를 통해 디지털포렌식 데이터를 수집하고자 하는 클라우드 기반 스토리지(300)에 연결되는 과정을 의미하며, 로그인은 클라우드 기반 스토리지(300)의 사용자로서 클라우드 기반 스토리지(300)를 이용할 수 있도록 로그인하는 것을 의미한다.

[0052] 보다 구체적으로, 로그인은 클라우드 기반 스토리지(300)의 사용자 아이디, 사용자 비밀번호, 사용자 인증 토큰 및 사용자 쿠키값 중 어느 하나 이상을 포함하는 사용자 크리덴셜(Credential)을 클라우드 기반 스토리지(30)로부터 수집하여 저장하고, 이를 통해 사용자의 자격으로서 이루어질 수 있으며, 보다 쉽게 이야기하면 장치(100)가 독립된 디바이스 중, 수사관의 전자 기기라면, 수사관의 전자 기기를 통해 클라우드 기반 스토리지(300)에 접근하여 실제 사용자 대신 수사관이 사용자의 자격으로 로그인을 수행하는 것으로 볼 수 있다.

[0053] 로그인을 수행했다면, 장치(100)가 로그인하여 수신한 응답으로부터 API(Application Programming Interface) 호출을 위한 공통인증정보를 추출한다(S320).

[0054] 여기서 공통인증정보는 클라우드 기반 스토리지(300)에 저장된 파일에 접근하기 위한, 보다 구체적으로 API 호출을 위해 필요한 정보로서, 클라우드 기반 스토리지(300)의 사용자 인증 토큰 및 사용자 쿠기값 중 어느 하나 이상일 수 있으며, 이와 같은 공통인증정보는 앞선 S310 단계에 따라 로그인을 수행함으로써 수신한 응답으로부터 추출할 수 있다.

[0055] 한편, API는 Application Programming Interface의 약자로서, 응용 프로그램이 운영 체제나 데이터베이스 관리 시스템 등과 같은 시스템 프로그램과 통신할 때 사용되는 언어나 메시지 형식을 가지며, 프로그램 내에서 실행을 위해 특정 서브루틴에 연결을 제공하는 함수를 호출하는 방식으로 구현될 수 있다.

[0056] 공통인증정보를 추출했다면, 장치(100)가 추출한 공통인증정보와 함께 제1 API 호출을 통해 클라우드 기반 스토리지(300)에 저장된 파일에 대한 목록 및 해당 목록이 포함하는 파일에 대한 메타데이터(Metadata)를 탐색한다(S330).

[0057] 여기서 제1 API는 클라우드 기반 스토리지(300)에 저장된 파일에 대한 목록 및 해당 목록이 포함하는 파일에 대한 메타데이터(Metadata)를 탐색하기 위한 API에 해당하며, 제1 API는 S320 단계에서 추출한 공통인증정보와 함께 클라우드 기반 스토리지(300)에 전송되어야 하는바, 공통인증정보를 함께 전송함으로써 클라우드 기반 스토리지(300)에 저장된 파일에 접근할 수 있는 권한, 보다 구체적으로 목록 및 해당 목록이 포함하는 파일에 대한 메타데이터를 탐색할 수 있는 권한을 부여 받을 수 있기 때문이다.

[0058] 한편, 클라우드 기반 스토리지(300)에 저장된 파일에 대한 목록은 클라우드 기반 스토리지(300)에 저장된 모든 파일을 전부 아우르는 목록이며, 해당 목록은 파일에 대한 다양한 정보를 포함할 수 있다. 그러나 이러한 목록에는 잠겨 있는 파일이 포함된 경우가 있을 수 있으며, 이 경우 해당 파일에 대한 메타데이터 탐색이 불가능할 수도 있는바, 이에 대해서는 후술하기로 한다.

[0059] 메타데이터는 데이터에 관한 구조화된 데이터로써 다른 데이터를 설명해주는 데이터인바, 그에 따라 S330 단계에서의 메타데이터는 클라우드 기반 스토리지에 저장된 파일의 파일명, 파일 크기, 파일 업로드 시간, 파일 수정 시간, 파일 삭제 시간, 파일을 공유 받은 자, 파일 작성자, 파일 히스토리, 썸네일, OCR, 조회수 및 조회자 중 하나 이상을 포함할 수 있으며, 파일에 따라 탐색되는 메타데이터의 세부적인 종류는 다를 수 있음은 물론이라 할 것이다.

[0060] 목록과 메타데이터까지 탐색했다면, 장치(100)가 추출한 공통인증정보와 함께 제2 API 호출을 통해 탐색한 목록 및 메타데이터에 대하여 수집을 위한 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하여 검색한다(S340).

[0061] 여기서 제2 API는 S330 단계에서 탐색한 클라우드 기반 스토리지(300)에 저장된 파일에 대한 목록 및 해당 목록이 포함하는 파일에 대한 메타데이터 내에서 수집을 위한 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하기 위한 API에 해당하며, 제2 API 역시 제1 API와 마찬가지로 S320 단계에서 추출한 공통인증정보와 함께 클라우드 기반 스토리지(300)에 전송되어야 하는바, 공통인증정보를 함께 전송함으로써 클라우드 기반 스토리지(300)에 저장된 파일에 접근할 수 있는 권한, 보다 구체적으로 수집을 위한 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하여 검색할 수 있는 권한을 부여 받을 수 있기 때문이다.

[0062] 한편, 수집을 위한 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하여 검색하면 되기 때문에 수집을 위한 기간만 적용하거나 또는 수집을 위한 키워드만을 적용하거나 또는 썸네일만을 적용할 수 있으며, 이들 셋 모두를 적용하여 검색할 수 있음은 물론이라 할 것인바, 이는 디지털포렌식 활동을 통해 수집하고자 하는 파일에 따라 적절하게 선택하여 검색을 진행할 수 있을 것이며, 일종의 검색 조건에 해당한다고 볼 수 있을 것이다.

[0063] 수집을 위한 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하여 검색까지 수행했다면, 마지막으로 장치(100)가 추출한 공통인증정보와 함께 제3 API 호출을 통해 클라우드 기반 스토리지(300)에 저장된 파일 중, 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일을 선별하여 수집을 시도한다(S350).

[0064] 여기서 제3 API는 S340 단계에서 수집을 위한 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하여 검색한 목록 및 메타데이터, 보다 구체적으로 검색 조건이 적용된 검색 결과에 대하여 해당 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일을 선별하여 수집을 시도하기 위한 API에 해당하며, 제3 API 역시 제1 API 및 제2 API와 마찬가지로 S320 단계에서 추출한 공통인증정보와 함께 클라우드 기반 스토리지(300)에 전송되어야 하는바, 공통인증정보를 함께 전송함으로써 클라우드 기반 스토리지(300)에 저장된 파일에 접근할 수 있는 권한, 보다 구체적으로 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일을 선별하여 수집할 수 있는 권한을 부여 받을 수 있기 때문이다.

[0065] 이와 같은 S350 단계는 도 4에 도시된 바와 같이 장치(100)가 검색 결과가 포함하는 메타데이터를 선별하여 수집하는 단계(S350-1) 및 장치(100)가 검색 결과가 포함하는 메타데이터에 해당하는 파일을 선별하여 수집하는 단계(S350-2)를 포함할 수 있는바, 검색 결과에 포함되는 메타데이터를 우선적으로 선별하여 수집하고, 이에 해당하는 파일만들 선별하여 수집하기 때문에 클라우드 기반 스토리지(300)에 저장된 파일 전부에 대한 디지털포렌식 활동이 필요하지 않게 되어 비용과 자원을 절감함으로써 효율성을 향상시킬 수 있으며, 디지털포렌식 활동을 통해 수집하고자 하는 데이터만을 선별하여 수집할 수 있기 때문에 피압수자의 프라이버시를 강화할 수 있다.

[0066] 한편, 검색 결과가 포함하는 메타데이터를 선별하여 수집한 후, 해당 메타데이터에 해당하는 파일을 선별하여 수집함에 있어서는 클라우드 기반 스토리지(300)에 저장된 파일에 대한 목록을 참조할 수 있는바, 앞서 설명한 바와 같이 목록에는 클라우드 기반 스토리지(300)에 저장된 모든 파일에 대한 다양한 정보를 포함하고 있기 때문이며, 이것이 앞선 S330 단계에서 클라우드 기반 스토리지(300)에 저장된 파일에 대한 목록을 탐색하는 그리고 S340 단계에서 목록에 수집을 위한 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하여 검색하는 하나의 이유가 될 수 있다 할 것이다.

[0067] 지금까지 본 발명의 제2 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법에 대하여 설명하였다. 본 발명에 따르면, 클라우드 기반 스토리지(300)에 저장된 모든 파일에 대하여 무분별한 디지털포렌식 활동을 수행하는 것이 아니라, 디지털포렌식 활동을 통해 수집하고자 하는 데이터를 선별하기 위한 검색 조건을 적용한 검색 결과에 포함되는 메타데이터 그리고 이에 해당하는 데이터만을 선별하여 수집하기 때문에 클라우드 기반 스토리지(300)에 저장된 파일 전부에 대한 디지털포렌식 활동이 필요하지 않게 되어 비용과 자원을 절감함으로써 디지털포렌식 활동의 효율성을 향상시킬 수 있다. 또한, 디지털포렌식 활동을 통해 수집하고자 하는 데이터를 선별하기 위한 검색 조건을 적용한 검색 결과에 포함되는 메타데이터 그리고 이에 해당하는 데이터만을 선별하여 수집하기에 클라우드 기반 스토리지(300)에 저장된 모든 데이터를 일률적으로 수집하지 않아도 되는바, 피압수자의 프라이버시를 강화할 수 있다.

[0068] 한편, 앞서 S330 단계에 대한 설명에서 목록에 잠겨있는 파일이 포함되는 경우가 있을 수 있다고 하며 이에 대한 설명을 보유한바, 이하 이에 관한 본 발명의 제3 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법에 대하여 설명하도록 한다.

[0069] 도 5는 본 발명의 제3 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법의 대표적인 단계를 나타낸 순서도이다.

[0070] 그러나 이는 본 발명의 목적을 달성함에 있어서 바람직한 실시 예일 뿐이며, 필요에 따라 일부 단계가 추가 또는 삭제될 수 있음은 물론이고, 어느 한 단계가 다른 단계에 포함되어 수행될 수도 있다.

[0071] 한편, S510 단계 내지 S530 단계는 앞서 설명한 본 발명의 제2 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법에서의 S310 단계 내지 S330 단계에 대한 설명과, S540 단계 내지 S550 단계는 앞서 설명한 S340 단계 내지 S550 단계에 대한 설명과 상당 부분 동일한바, 중복 서술을 방지하기 위해 자세한 설명은 생략하도록 하며, 이하 차이점에 대해서만 설명하도록 한다.

[0072] 클라우드 기반 스토리지(300)에 저장된 파일에 대한 목록 및 해당 목록이 포함하는 파일에 대한 메타데이터를 탐색하였을 때, 목록에는 잠겨 있는 파일이 포함될 수 있으며, 이 경우 파일이 잠겨있기 때문에 해당 파일에 대한 메타데이터 탐색이 불가능할 수 있는바, 그렇다하여 디지털포렌식 활동에서 의도적으로 제외할 수는 없을 것이며, 잠겨있는 파일인만큼 중요한 파일일 가능성이 높기 때문에 디지털포렌식 활동을 통해 수집하고자 하는 데이터를 선별하기 위한 검색 조건을 적용시켜볼 필요성이 있다.

[0073] 따라서 클라우드 기반 스토리지(300)에 저장된 파일에 대한 목록 및 해당 목록이 포함하는 파일에 대한 메타데이터를 탐색한 후, 장치(100)가 탐색한 목록 및 메타데이터에 대하여 수집을 위한 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하여 검색하기 위해 추가인증정보가 필요한지 판단한다(S535).

[0074] 여기서 추가인증정보는 잠겨있는 파일을 풀 수 있는 인증정보를 의미하며, 앞서 설명한 공통인증정보와 동일한 인증정보일 수도 있고 또는 이와 상이한 인증정보일 수도 있을 것이다.

[0075] 추가인증정보가 필요한지 판단하는 S535 단계는 결국 S530 단계에서 탐색한 목록에 잠겨 있는 파일이 포함되어 있는지 여부를 판단하는 것으로 볼 수 있는바, 판단 결과 감겨 있는 파일이 포함되어 있지 않아 추가인증정보가 필요하지 않다고 판단하는 경우, S540 단계로 넘어가게 되며, S540 단계는 앞서 설명한 S340 단계와 동일함은 이미 밝혀둔바 있다.

[0076] 한편, S535 단계에 대한 판단 결과 잠겨 있는 파일이 포함되어 있어 추가인증정보가 필요하다고 판단하는 경우, 장치(100)가 클라우드 기반 스토리지(300)에 추가인증정보를 호출하여 확보하며(S537), 그 이후 장치(100)가 확보한 추가인증정보와 함께 제K(여기서 K는 4 이상의 자연수) API 호출을 통해 클라우드 기반 스토리지(300)에 저장된 파일에 대한 목록′ 및 해당 목록′ 이 포함하는 파일에 대한 메타데이터′ 를 재탐색한다(S539).

[0077] 여기서 제K API는 클라우드 기반 스토리지(300)에 저장된 파일에 대한 목록′ 및 해당 목록′ 이 포함하는 파일에 대한 메타데이터′ 를 탐색하기 위한 API에 해당하며, S530 단계와 같이 목록과 메타데이터가 아니라 목록′

과 메타데이터 ′ 인 것은 잠겨 있던 파일의 잠김을 풀 수 있는 추가인증정보를 확보하여 함께 전송함으로써 기존에 잠겨 있던 파일의 잠김이 풀어져 있는 상태에서의 새로운 목록′ 과 해당 목록′ 이 포함하는 파일에 대한 메타데이터이기′ 에 기존의 목록과 메타데이터와 구분하기 위함이다.

[0078] 따라서 S530 단계에서의 목록과 S539 단계에서의 목록′ 은 S530 단계에서 잠겨 있던 파일이 S539 단계에서는 풀어져 있는 상태의 파일로 포함되어 있는 것을 제외하고, 나머지 파일에 대한 사항은 동일하다고 할 것이며, 메타데이터의 경우 S530 단계에서 잠겨 있던 파일에 대한 메타데이터는 탐색이 불가능했으나 S539 단계에서는 잠겨 있던 파일이 풀어져 있는 상태로 목록′ 에 포함되기에, 해당 파일′ 에 대한 메타데이터 ′ 역시 탐색이 가능하다고 할 것이며, 나머지 파일에 대한 메타데이터에 관한 사항은 동일하다고 할 것이다.

[0079] 한편, S539 단계를 통해 목록′ 및 메타데이터′ 가 재탐색되었으므로, 그 이후인 S540 단계에서의 목록은 목록 ′ 으로, S540 단 및 S550 단계에서의 메타데이터 역시 메타데이터′ 로, 공통인증정보는 추가인증정보로 대체된다 할 것이다.

[0080] 아울러, S535 단계 내지 S539 단계에 대한 설명은 잠겨 있던 파일을 출기 위한 추가인증정보가 하나인 것을 전제로 한 것이며, 잠겨 있던 파일이 복수 개이며, 각각의 파일을 풀기 위한 추가인증정보 역시 복수 개인 경우, 모든 파일에 대한 잠김을 풀 때까지 S535 단계 내지 S539 단계가 반복하여 수행되거나, 장치(100)의 프로세서(10)를 병렬 프로세싱이 가능한 프로세서로 구현한 경우, 병렬 프로세싱을 통해 동시 다발적으로 수행될 수 있음은 물론이라 할 것이다.

[0081] S539 단계를 통해 목록′ 과 메타데이터′ 까지 재탐색했다면, 장치(100)가 확보한 추가인증정보와 함께 제2 API 호출을 통해 재탐색한 목록′ 및 메타데이터′ 에 대하여 수집을 위한 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하여 검색하며(S540), 확보한 추가인증정보와 함께 제3 API 호출을 통해 클라우드 기반 스토리지(300)에 저장된 파일 중, 검색 결과가 포함하는 메타데이터′ 및 이에 해당하는 파일을 선별하여 수집을 시도한다(S550).

[0082] S540 단계 및 S550 단계와 본 발명의 제2 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법에서의 S340 단계 및 S350 단계의 차이점은 잠겨 있던 파일을 풀기 위해 추가인증정보를 획득하였으므로 기존의 공통인증정보가 아닌 새롭게 획득한 추가인증정보를 제2 API 호출(S540 단계의 경우) 또는 제3 API 호출(S550 단계의 경우)과 함께 전송한다는 점과 수집을 위한 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하여 검색하는 목록이 잠겨 있던 파일이 풀어져 있는 상태에서의 목록인 목록′ 이라는 점, 메타데이터가 역시 잠겨 있던 파일이 풀어져 있는 상태에서의 목록′ 이 포함하는 파일에 대한 메타데이터′ 라는 점이라 할 것이다.

[0083] 지금까지 본 발명의 제3 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법에 대하여 설명하였다. 본 발명에 따르면, 클라우드 기반 스토리지(300)에 저장된 파일 중, 잠겨 있는 파일이 존재하더라도 이에 대한 잠김을 풀 수 있는 추가인증정보를 획득하여 잠김을 푼 후, 잠김이 풀어져 있는 상태의 파일을 포함하는 새로운 목록 및 해당 새로운 목록이 포함하는 파일에 대한 메타데이터를 재탐색하기 때문에 클라우드 기반 스토리지(300)에 저장되어 있는 데이터의 누락 없이 디지털포렌식 활동의 정확도를 향상시킬 수 있다.

[0084] 이번에는 본 발명의 제2 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법에서 S350 단계를 통해 또는 본 발명의 제3 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법에서 S550 단계를 통해 파일을 선별하여 수집을 시도함에도 불구하고 파일이 적합하게 수집되지 않는 경우에 관한 본 발명의 제4 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법에 대하여 설명하도록 한다.

[0085] 도 6은 본 발명의 제4 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법의 대표적인 단계를 나타낸 순서도이다.

[0086] 그러나 이는 본 발명의 목적을 달성함에 있어서 바람직한 실시 예일 뿐이며, 필요에 따라 일부 단계가 추가 또는 삭제될 수 있음은 물론이고, 어느 한 단계가 다른 단계에 포함되어 수행될 수도 있다.

[0087] 한편, S610 단계 내지 S650 단계는 앞서 설명한 본 발명의 제2 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법에서의 S310 단계 내지 S350 단계에 대한 설명과 동일한바, 중복 서술을 방지하기 위해 자세한 설명은 생략하도록 하며, 이하 차이점에 대해서만 설명하도록 한다.

[0088] 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일을 선별하여 수집을 시도한 후, 장치(100)는 클라우드 기반 스토리지로부터 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일이 수집되었는지 판단한다(S660).

[0089] 여기서 수집은 일부가 아니라 전부를 의미하는바, 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일의 일부라도 수집되지 않았다면 다음과 같은 S670 단계가 수행되며(NO), 전부 수집된 경우(YES)에만 프로세스가 종료될 수 있을 것이다.

[0090] S660 단계에서의 판단 결과 수집되지 않았다면, 장치(100)가 제3 API 호출에 대하여 수신한 응답으로부터 제N (여기서 N은 4 이상의 자연수) API를 추출하며(S670), 추출한 공통인증정보와 함께 제N API 호출을 통해 클라우드 기반 스토리지(300)에 저장된 파일 중, 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일을 선별하여 수집을 시도한다(S680).

[0091] 이는 쉽게 설명하면, 수집되지 않은 파일을 수집하기 위한 API를 다시 추출하여 수집을 시도한다는 것이며, S680 단계 이후에는 제N API를 제N+1 API로 대체하여(S690) S660 단계로 회귀하는바, 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일이 전부 수집될 때까지 이상의 단계들이 반복된다 할 것이다.

[0092] 지금까지 본 발명의 제4 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법에 대하여 설명하였다. 본 발명에 따르면, 클라우드 기반 스토리지(300)에 저장된 파일 중, 디지털포렌식 활동을 통해 수집하고자 하는 데이터를 선별하기 위한 검색 조건을 적용한 검색 결과에 포함되는 메타데이터 그리고 이에 해당하는 데이터 중 일부라도 수집되지 않는다면, 수집을 위한 API를 재호출하여 지속적으로 수집을 시도할 수 있는바, 수집이 필요한 데이터임에도 불구하고 수집하지 못하게 되는 상황을 방지할 수 있음으로써 디지털포렌식 활동의 정확도를 향상시킬 수 있다.

[0093] 지금까지 도 2 내지 도 6을 참조하며 본 발명의 제 2 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법 내지 제4 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법에 대하여 설명하였다. 이들 모두 클라우드 기반 스토리지(300)를 대상으로 하는바, 클라우드 기반 스토리지 서비스의 종류에 따라 한 번의 로그인이 아니라 2차 인증까지 필요한 경우도 존재하는바, 그에 따라 이들 모든 실시 예는 로그인하는 단계(S310, 510, 610 단계)와 공통인증정보를 추출하는 단계(S320, 520, 620) 사이에 장치(100)가 로그인한 클라우드 기반 스토리지(300)가 2차 인증이 필요한지 판단하는 단계(S315) 및 판단 결과 2차 인증이 필요하다면, 클라우드 기반 스토리지(300)로부터 인증 메시지 및 인증 코드 중 어느 하나 이상을 수신하여 2차 인증을 수행하는 단계(S317)를 더 포함할 수 있으며, 이를 도 7에 본 발명의 제 2 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법 에 대한 도 3을 기준으로 S315 단계 및 S317 단계를 추가한 본 발명의 제 5 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법의 대표적인 단계를 나타낸 순서도로 예시적으로 도시하였다.

[0094] 한편, 본 발명의 제1 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 장치(100)는 도 1과 같은 모습뿐만 아니라 도 8에 예시적으로 도시한 바와 같이 각각의 기능을 수행하는 기능적인 구성을 포함하는 장치(1000)로 나타낼 수도 있으며, 본 발명의 제1 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 장치(100)와 본 발명의 제2실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법 내지 본 발명의 제5실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법은 모든 기술적 특징을 동일하게 포함하는 본 발명의 제6 실시 예에 따른 컴퓨터로 판독 가능한 매체에 저장된 컴퓨터 프로그램으로 구현할 수도 있는바, 이 경우 컴퓨팅 장치와 결합하여, (AA) 클라우드 기반 스토리지에 접속하여 로그인하는 단계, (BB) 상기 로그인하여 수신한 응답으로부터 API(Application Programming Interface) 호출을 위한 공통인증정보를 추출하는 단계, (CC) 상기 추출한 공통인증정보와 함께 제1 API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일에 대한 목록 및 상기 목록이 포함하는 파일에 대한 메타데이터(Metadata)를 탐색하는 단계, (DD) 상기 추출한 공통인증정보와 함께 제2 API 호출을 통해 상기 탐색한 목록 및 메타데이터에 대하여 수집을 위한 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하여 검색하는 단계 및 (EE) 상기 추출한 공통인증정보와 함께 제3 API 호출을 통해 상기 클라우드 기반 스토리지에 저장된 파일 중, 상기 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일을 선별하여 수집을 시도하는 단계를 실행할 수 있을 것이며, 중복 서술을 위해 자세히 기재하지는 않았지만 본 발명의 제1 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 장치(100) 및 본 발명의 제2 실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법 내지 본 발명의 제5실시 예에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법에 적용된 모든 기술적 특징은 본 발명의 제6 실시 예에 따른 컴퓨터로 판독 가능한 매체에 저장된 컴퓨터 프로그램에 모두 동일하게 적용될 수 있음은 물론이라 할 것이다.

[0095] 이상 첨부된 도면을 참조하여 본 발명의 실시 예들을 설명하였지만, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될

수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시 예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다.

부호의 설명

[0096] 10: 프로세서

20: 네트워크 인터페이스

30: 메모리

40: 스토리지

41: 컴퓨터 프로그램

50: 정보 버스

100, 1000: 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 장치

200: 클라우드 기반 스토리지

300: 네트워크

1100: 원격지 서버 접근부

1200: 인증정보 추출부

1300: API 호출부

1310: 데이터 탐색부 1320: 검색부 1330: 데이터 선별부

1400: 수집부

1410: 메타데이터 수집부 1420: 썸네일 수집부

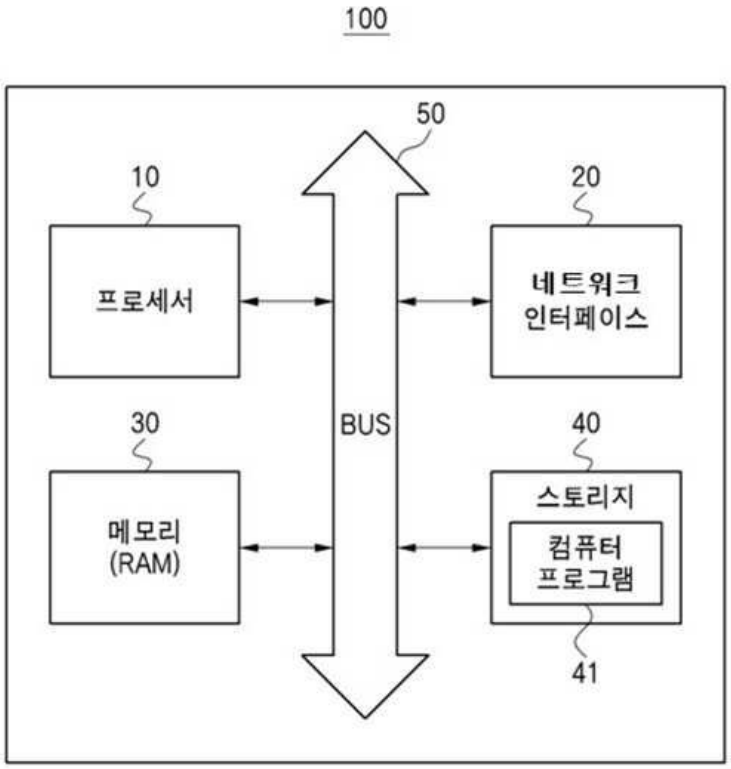
1430: 파일 히스토리 수집부 1440: 컨텐츠 수집부

200: 클라우드 기반 스토리지

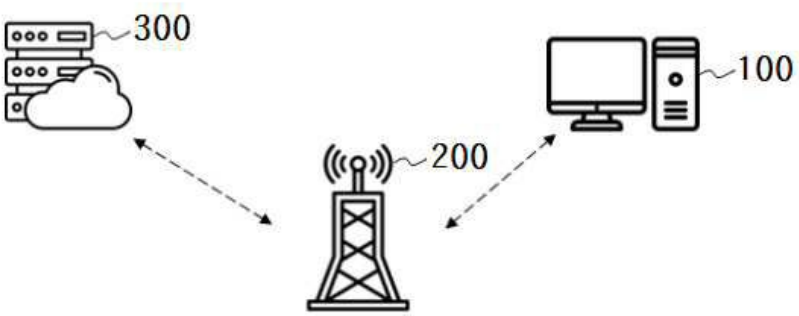
300: 네트워크

도면

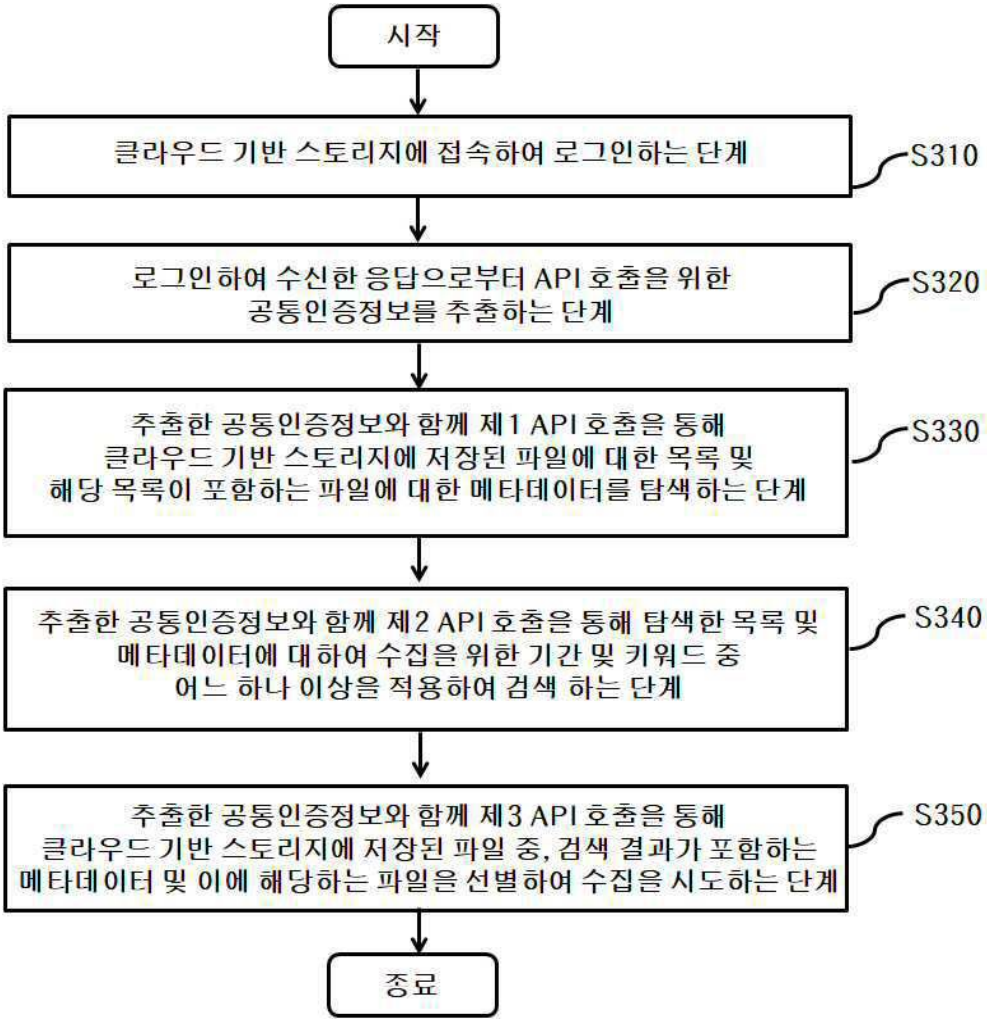
도면1


100
50
10
프로세서
20
네트워크
인터페이스
30
메모리
(RAM)
BUS
40
스토리지
컴퓨터
프로그램
41

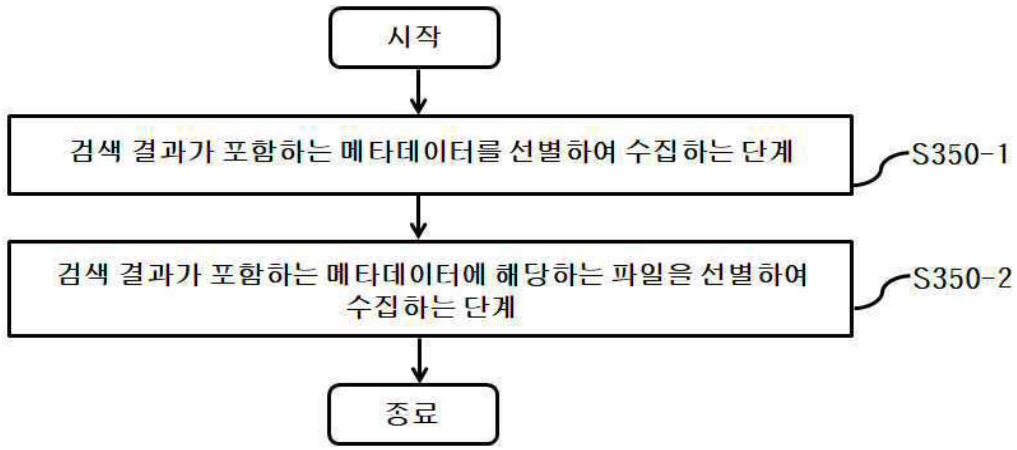
도면2


300
100
200

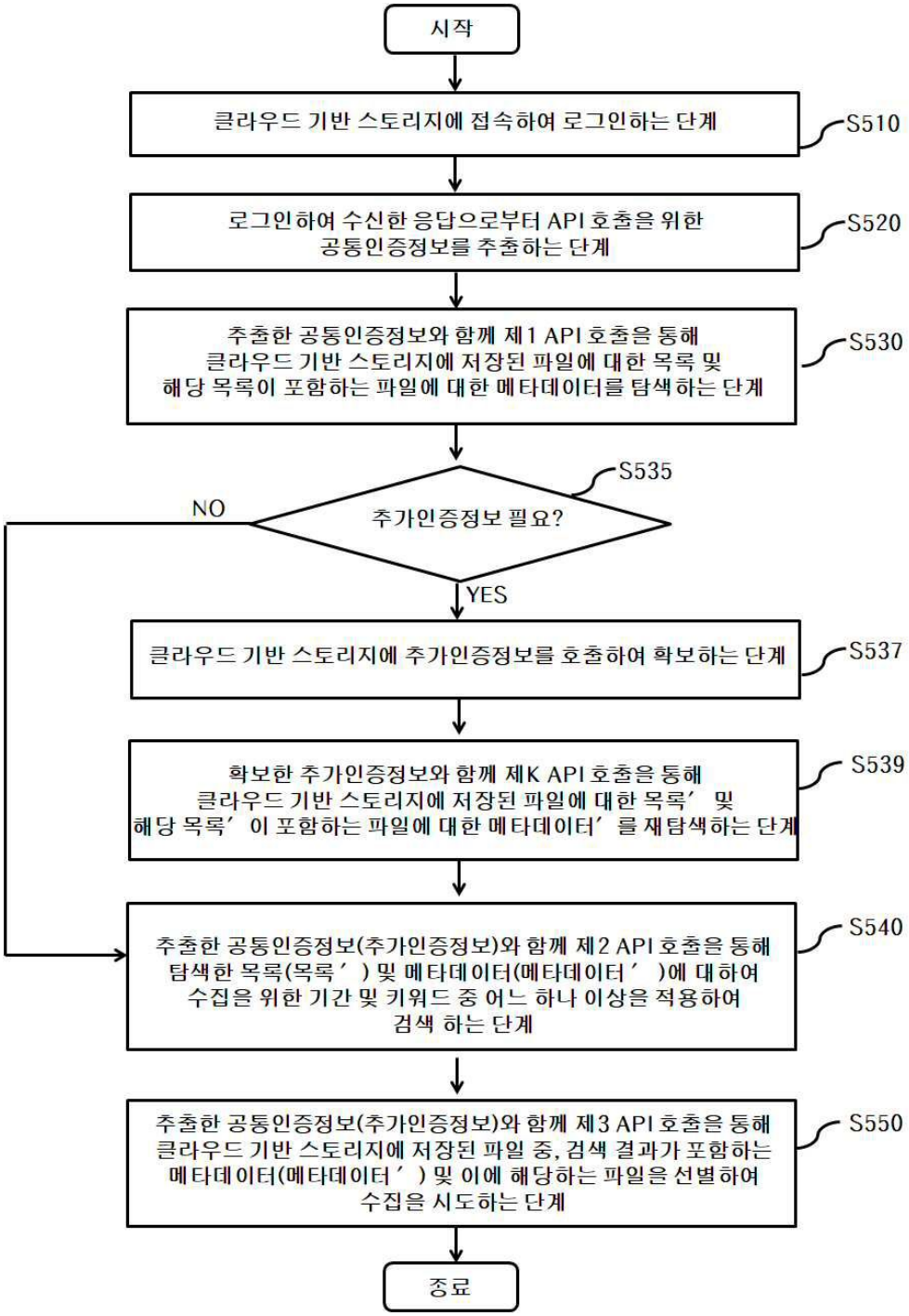
도면3


시작
클라우드 기반 스토리지에 접속하여 로그인하는 단계
S310
로그인하여 수신한 응답으로부터 API 호출을 위한
공통인증정보를 추출하는 단계
S320
추출한 공통인증정보와 함께 제1 API 호출을 통해
클라우드 기반 스토리지에 저장된 파일에 대한 목록 및
해당 목록이 포함하는 파일에 대한 메타데이터를 탐색하는 단계
S330
추출한 공통인증정보와 함께 제2 API 호출을 통해 탐색한 목록 및
메타데이터에 대하여 수집을 위한 기간 및 키워드 중
어느 하나 이상을 적용하여 검색 하는 단계
S340
추출한 공통인증정보와 함께 제3 API 호출을 통해
클라우드 기반 스토리지에 저장된 파일 중, 검색 결과가 포함하는
메타데이터 및 이에 해당하는 파일을 선별하여 수집을 시도하는 단계
S350
종료

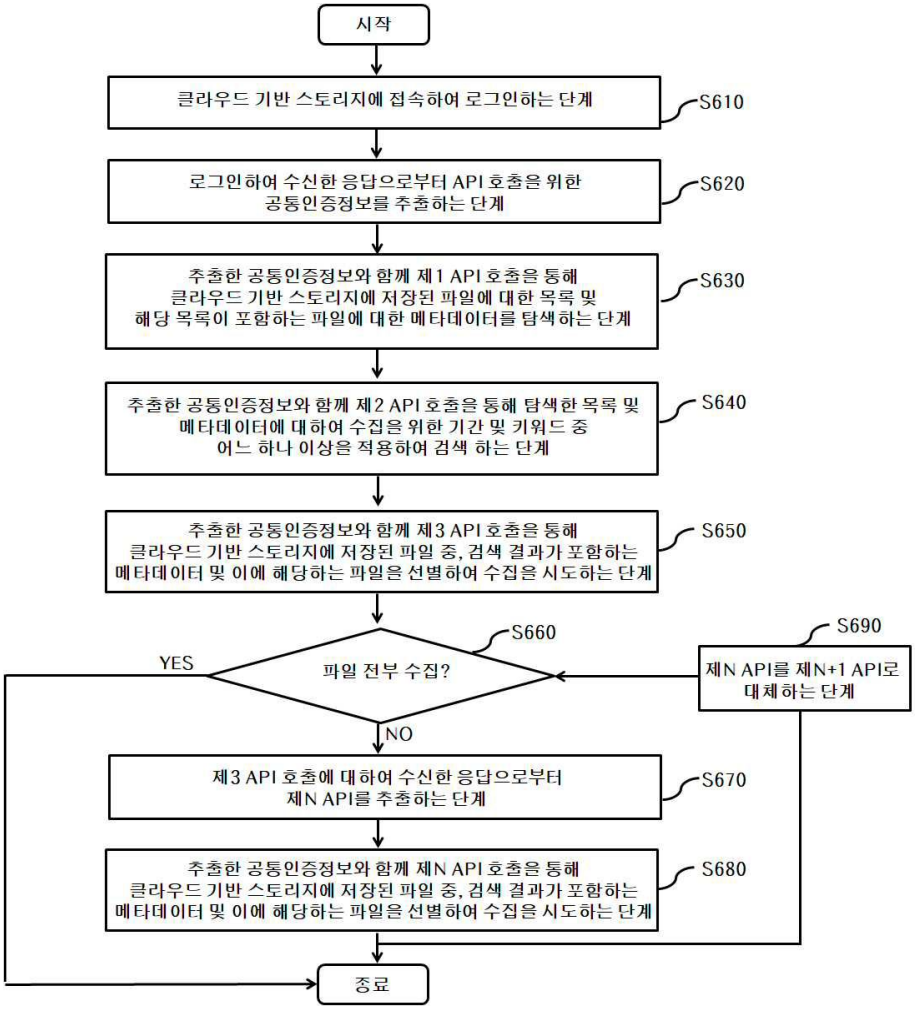
도면4


시작
검색 결과가 포함하는 메타데이터를 선별하여 수집하는 단계
S350-1
검색 결과가 포함하는 메타데이터에 해당하는 파일을 선별하여
수집하는 단계
S350-2
종료

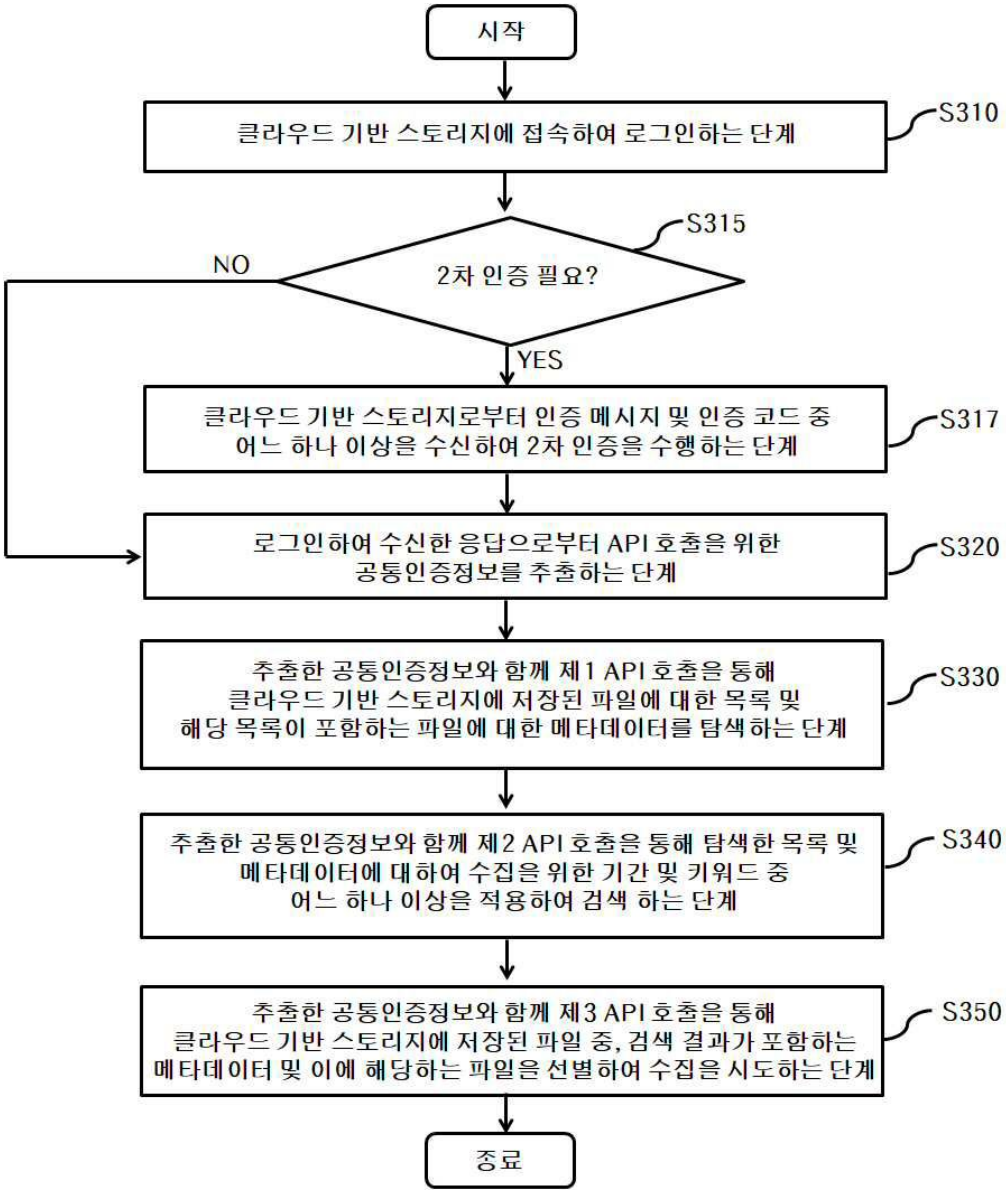
도면5


시작
클라우드 기반 스토리지에 접속하여 로그인하는 단계
S510
로그인하여 수신한 응답으로부터 API 호출을 위한
공통인증정보를 추출하는 단계
S520
추출한 공통인증정보와 함께 제1 API 호출을 통해
클라우드 기반 스토리지에 저장된 파일에 대한 목록 및
해당 목록이 포함하는 파일에 대한 메타데이터를 탐색하는 단계
S530
S535
추가인증정보 필요?
NO
YES
클라우드 기반 스토리지에 추가인증정보를 호출하여 확보하는 단계
S537
확보한 추가인증정보와 함께 제K API 호출을 통해
클라우드 기반 스토리지에 저장된 파일에 대한 목록′ 및
해당 목록′ 이 포함하는 파일에 대한 메타데이터′ 를 재탐색하는 단계
S539
추출한 공통인증정보(추가인증정보)와 함께 제2 API 호출을 통해
탐색한 목록(목록′) 및 메타데이터(메타데이터′)에 대하여
수집을 위한 기간 및 키워드 중 어느 하나 이상을 적용하여
검색 하는 단계
S540
추출한 공통인증정보(추가인증정보)와 함께 제3 API 호출을 통해
클라우드 기반 스토리지에 저장된 파일 중, 검색 결과가 포함하는
메타데이터(메타데이터′) 및 이에 해당하는 파일을 선별하여
수집을 시도하는 단계
S550
종료

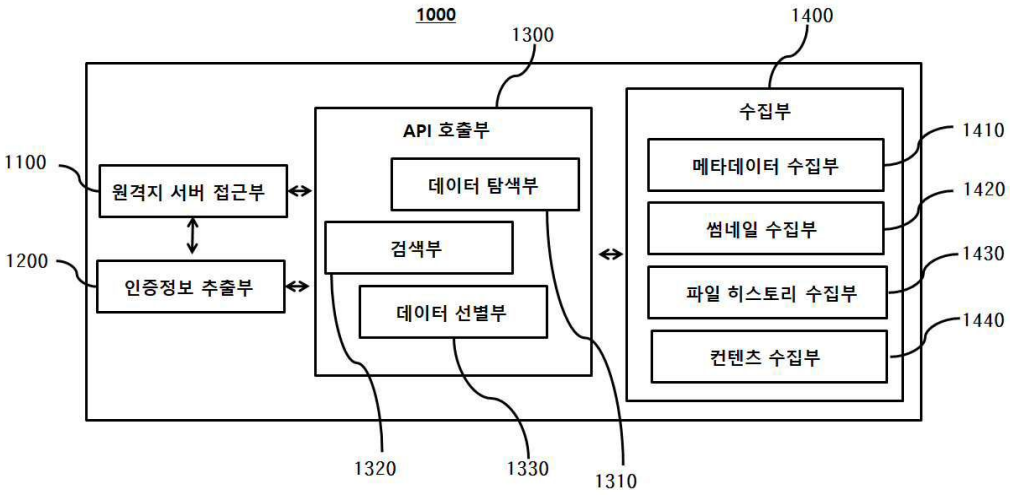
도면6


시작
클라우드 기반 스토리지에 접속하여 로그인하는 단계
S610
로그인하여 수신한 응답으로부터 API 호출을 위한
공통인증정보를 추출하는 단계
S620
추출한 공통인증정보와 함께 제1 API 호출을 통해
클라우드 기반 스토리지에 저장된 파일에 대한 목록 및
해당 목록이 포함하는 파일에 대한 메타데이터를 탐색하는 단계
S630
추출한 공통인증정보와 함께 제2 API 호출을 통해 탐색한 목록 및
메타데이터에 대하여 수집을 위한 기간 및 키워드 중
어느 하나 이상을 적용하여 검색 하는 단계
S640
추출한 공통인증정보와 함께 제3 API 호출을 통해
클라우드 기반 스토리지에 저장된 파일 중, 검색 결과가 포함하는
메타데이터 및 이에 해당하는 파일을 선별하여 수집을 시도하는 단계
S650
S660
파일 전부 수집?
YES
NO
S690
제N API를 제N+1 API로
대체하는 단계
제3 API 호출에 대하여 수신한 응답으로부터
제N API를 추출하는 단계
S670
추출한 공통인증정보와 함께 제N API 호출을 통해
클라우드 기반 스토리지에 저장된 파일 중, 검색 결과가 포함하는
메타데이터 및 이에 해당하는 파일을 선별하여 수집을 시도하는 단계
S680
종료

도면7


시작
클라우드 기반 스토리지에 접속하여 로그인하는 단계
S310
S315
2차 인증 필요?
NO
YES
클라우드 기반 스토리지로부터 인증 메시지 및 인증 코드 중 어느 하나 이상을 수신하여 2차 인증을 수행하는 단계
S317
로그인하여 수신한 응답으로부터 API 호출을 위한 공통인증정보를 추출하는 단계
S320
추출한 공통인증정보와 함께 제1 API 호출을 통해 클라우드 기반 스토리지에 저장된 파일에 대한 목록 및 해당 목록이 포함하는 파일에 대한 메타데이터를 탐색하는 단계
S330
추출한 공통인증정보와 함께 제2 API 호출을 통해 탐색한 목록 및 메타데이터에 대하여 수집을 위한 기간 및 키워드 중 어느 하나 이상을 적용하여 검색 하는 단계
S340
추출한 공통인증정보와 함께 제3 API 호출을 통해 클라우드 기반 스토리지에 저장된 파일 중, 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일을 선별하여 수집을 시도하는 단계
S350
종료

도면8


1000
1300
1400
API 호출부
데이터 탐색부
검색부
데이터 선별부
수집부
메타데이터 수집부
썸네일 수집부
파일 히스토리 수집부
컨텐츠 수집부
1410
1420
1430
1440
1100
원격지 서버 접근부
1200
인증정보 추출부
1320
1330
1310