

속성 정보를 이용한 파일 검색 장치 및 방법

■ **보유기관** 한국전자통신연구원

■ **주요 발명자** 길연희 | 이주영 | 조수형

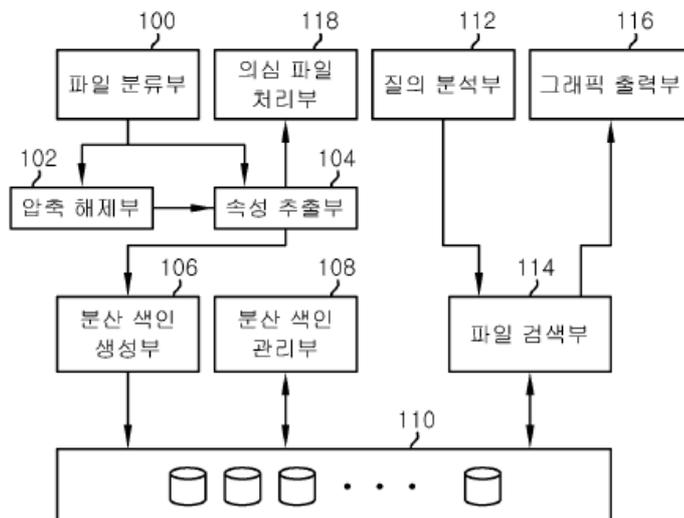
■ 권리사항	
· 출원번호	10-2011-0129062
· 출원일	2011년 12월 05일
· 현재상태	<input type="checkbox"/> 등록 <input checked="" type="checkbox"/> 공개 <input type="checkbox"/> 미공개
■ 기술완성도	<input type="checkbox"/> 기초연구단계 <input checked="" type="checkbox"/> 실험단계 <input type="checkbox"/> 시작품단계 <input type="checkbox"/> 제품화단계

■ **적용가능분야 및 목표시장** E-Discovery 등 디지털 포렌식 응용 분야

■ 기술 개요

분산 포렌식 인덱스 검색 기술' 이란 수사의 대상이 되는 디지털 데이터에 대한 빠른 검색을 제공하기 위해 분산 처리 기법으로 인덱스를 생성해 두었다가 사용자 요청이 있을 경우, 인덱스에서 찾아 검색 결과를 실시간으로 전송하는 기술임

■ 기술 개념도



[그림] 파일 검색 장치 블록도

■ 기술 내용 및 동향

□ 기술의 특징

[고객/시장의 니즈를 충족시키는 독특한 점]

- ▷ 분산 인덱싱 수행 시 안정성 제공 및 분산 환경 관리를 위해 Apache Hadoop 프레임워크를 기반으로 개발됨
- ▷ Hadoop을 기반으로 개발되어 Scalability가 높고, Amazon EC2, S3에 기반하는 Amazon Elastic MapReduce과 같은 클라우드 컴퓨팅 환경으로 쉽게 이식되어 수행될 수 있음
- ▷ 국내외 다양한 형태의 파일내용 및 메타데이터를 추출할 수 있는 포렌식 파일 필터를 제공함

[기술의 상세 사양]



[경쟁기술/대체기술 현황]

- ▷ 현재 상용화되어 있는 컴퓨터 포렌식 소프트웨어는 Guidance Software사의 EnCase, Technology Pathways사의 ProDiscover, AccessData사의 FTK, ASR Data사의 SMART 등이 있으며, EnCase Edition이 가장 높은 시장 점유율을 차지하고 있음
- ▷ 그 중 FTK는 분산 인덱스 검색 기술을 제공하고 있으나 한국어 및 국산소프트웨어로 생성된 문서에 대한 지원이 제대로 이루어지지 않고 있으며, 해당 기능을 구매에 고가의 비용이 소요됨

■ 관련 기술

1	출원번호	10-2011-0114168
	발명의 명칭	분산 처리를 이용한 포렌식 인덱스 방법 및 장치
2	출원번호	10-2011-0129062
	발명의 명칭	속성 정보를 이용한 파일 검색 장치 및 방법

■ 시장 동향

□ 해당 제품/서비스 시장 규모

- ▷ 디지털 포렌식 SW 및 서비스 시장을 포함하는 Legal Discovery의 SW 시장 ' 14년 약 80,058억 원 전망(연평균 11%대 성장률, 환율 1,200원 적용)
- ▷ 국내 시장 규모는 ' 14년 1,201억원으로 성장 예측 (세계시장의 1.5% 수준)

[표 1] 세계 Legal Discovery Software 시장 (단위: 백만원)

구분	2010	2014	2016
세계 시장 규모	5,111,000	7,885,700	9,715,900
국내 시장 규모	77,800	120,100	147,960

□ 해당 제품/서비스 시장 국내외 동향

- ▷ 국내 포렌식 분석 기술의 경우, 한국전자통신연구원이 다양한 고급 분석 기능을 탑재한 한국형 디지털 포렌식 시스템을 개발한 바 있고, 하드디스크 복구 전문 업체인 파이널데이터사도 파일 복구 기술에 대한 특허를 보유하고 이를 통해 몇몇 제품을 이미 출시한 상태이나, 대용량 데이터에 대한 특화된 기술이나 디지털 증거 시각화 분석 기술 등의 고급 분석 기술 개발은 아직 미비한 상태임
- ▷ 디지털 포렌식 도구를 상용화한 국가 중 가장 큰 기술력과 시장규모를 가지고 있는 국가는 미국이며, 영국, 프랑스, 러시아 등도 분야별로 디지털 포렌식 기술을 독자 개발 중에 있음
- ▷ IDC에 따르면 전 세계의 데이터량은 2010년 ZB시대로 진입했으며, 전 세계의 데이터량의 70%가 개인으로부터 발생함을 추정함 이에 따라 포렌식적인 대응책에 대한 연구 및 기술개발이 활발히 진행 중에 있음

■ 문의처

· 소속	사업화본부 기술이전팀
· 담당자	김호민 기술원
· 연락처	042-860-1804, hominkim@etri.re.kr