Smart & Green Technology Innovator

4-2 SNS 포렌식 데이터 시각화 기술

본 기술은 포렌식적인 목적으로 SNS 데이터를 활용하여 용의자와 주변인 간의 인적관계 파악, 대화내용 추적 등이 가능함. 또한 수집된 SNS 데이터(Facebook)를 분석이 용이한 시각화 데이터로 변형하고, 1인이 아닌 다수의 인물에 대한 소셜 연관관계 도출하여 국가 사법 기관의 국가 과학수사 기술력 증대 및 컴퓨터 범죄, 해킹, 회사기밀 유출 등 컴퓨터, 사이버 범죄에 대한 효율적 분석 수단법 제공함

암호기술연구팀 담당자 김건우

ETRI 한국전자통신연구원
Electronics and Telecommunications Research Institute

목 차

1. 기술 개요(1)

기술개발의 필요성

고객 및 시장의 니즈

- 과거에 커뮤니티 중심으로 온라인상에서 활동하던 유저들이 개인을 중심으로 한 SNS로 이동해옴에 따라 이를 통해 생성, 전파되는 대용량 데이터를 분석함으로써 각 개인 또는 그룹 내 영향력, 관심사, 성향 및 행동패턴을 분석하는 소셜 네트워크 분석은 다양한 분야에서 활용되고 있음

- 포렌식적인 목적으로는 SNS 데이터를 활용하여 용의자와 주변인 간의 인적관계 파악, 대화내용 추적 등이 가능하며, 최근 미국에서 facebook, My Space, twitter, linkedIn 등의 소셜 네트워크 서비스에서 획득된 정보가 법정에서 증거로 채택되고 있음

- SNS 포렌식 데이터 시각화는 방대한 SNS 데이터를 이용해 분석이 용이한 형상으로 도시화함으로써 단순한 데이터 나열만으로는 볼 수 없었던 정보를 제시할 수 있음

- SNS 데이터를 분석 대상자 간의 커뮤니케이션 채널로 이해하고, 이를 기존의 커뮤니케이션 분석과 연계하여 연관관계 및 통신내역 분석 시각화 기능이 요구됨

1. 기술 개요(2)

기술개념 및 기술사양

기술개념

- 수집된 SNS 데이터(Facebook)를 분석이 용이한 시각화 데이터로 변형
- 1인이 아닌 다수의 인물에 대한 소셜 연관관계 도출
  - N명의 소셜 사용자간의 숨어있는 커뮤니케이션 분석
- 연관성을 시각화 기법을 통해 표현함으로 의미 있는 포렌식 정보 제공
- SNS 이벤트 타임라인 제공

기술구성도

- SNS 포렌식 데이터 수집 시스템
  - Web 기반 SNS 포렌식 데이터 수집
  - SNS 포렌식 데이터 공통 데이터 컨테이너
- SNS 포렌식 데이터 시각화 분석 시스템
  - Dynamic Graph Modeling 시스템
  - SNS Data Timeline Modeling 시스템

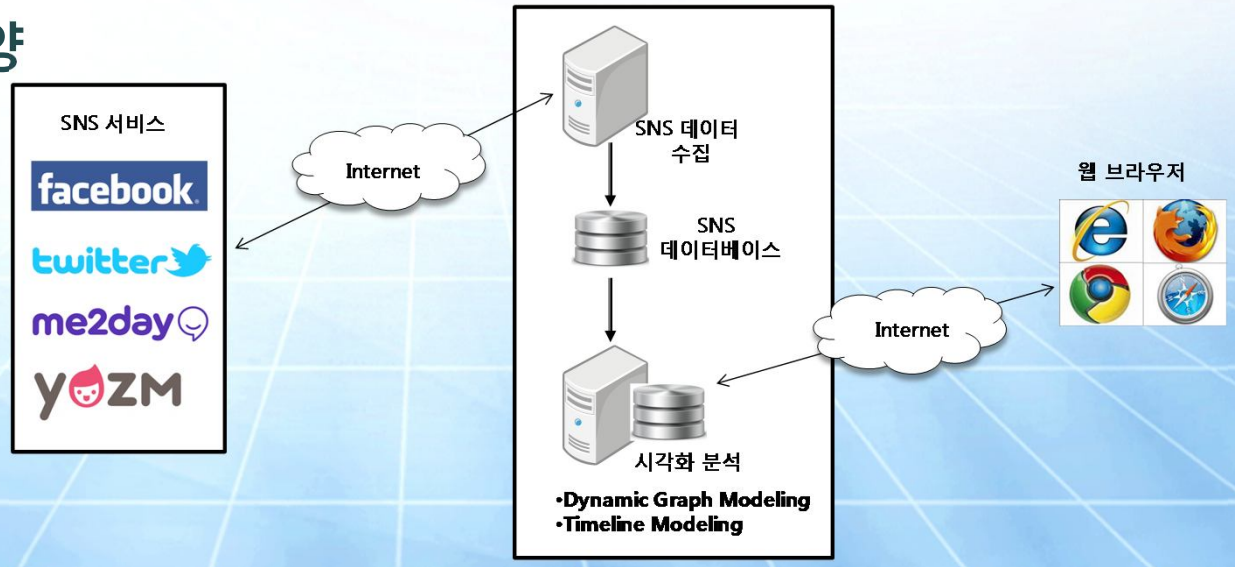
2. 개발기술의 주요내용(1)

기술의 특징

고객/시장의 니즈를 충족시키는 독특한 점

- SNS 포렌식 수집도구와 시각화 분석도구를 분리하여 각각 기술이전 및 통합이전 가능
- SNS 상호작용 데이터 분석 결과를 이해하기 쉬운 그래프로 표현
- 하나의 시각화 분석 도구를 사용하여 복수의 SNS 사용자 간의 데이터 분석 가능
- 통합 분석을 위한 공통 데이터 포맷을 제공하여 페이스북 뿐만 아니라 카카오톡 및 기타 SMS 데이터 파일(CSV) 등을 로드하여 통합 분석 가능
- 수집되는 SNS 데이터 이벤트가 다양하고 시간대 별로 사용자 행위 표현 가능
- 시각화 분석시 사용자에 의한 데이터 필터링에 의해 행위의 세부 분석 가능

기술의 상세 사양



2. 개발기술의 주요내용(2)

경쟁기술대비 우수성

경쟁기술/대체기술 현황

- 경쟁기술은 다수의 SNS 사용자간의 상호관계에 대한 분석을 지원하지 않음
- 데이터 수집에 중점을 두고 있어 통계정보, 인적관계 분석, 통합 분석을 지원하지 않음
- 연간 라이선스 비용 등의 유지비용이 높음
- 행위 분석을 위해서 기존 기술은 사용법이 어렵고 인터페이스가 복잡함

경쟁기술/대체기술 대비 우수성

경쟁기술	•본 기술의 우수성
• i2 Analyst Notebook - 증거 데이터중 단일 SNS 사용자 데이터 시각화에 적합 - 복잡한 유저 인터페이스와 도구 조작의 어려움	- 웹 기반 동작방식으로 동시에 여러명의 분석관이 동시에 사용가능함 - SNS 데이터 수집과 시각화 분석을 분리하여 사용 편의성을 높임 - 수집된 SNS 데이터에 대한 통계정보, 인적관계 분석, 통합 분석 지원 - Keyword 검색, 데이터간의 interaction 계산 가능 - 포렌식 도구 사용자가 분석을 용이하게 하기 위해 타겟 인물들을 병합하여 하나의 동일 인물로 설정하거나 관련없는 인물들을 삭제 가능함

2. 개발기술의 주요내용(3)

기술의 완성도

기술개발 완료시기

- 2014년 02월

기술이전 범위

- SNS 포렌식 데이터 수집 기술
  - 클라이언트/서버 기반의 SNS 데이터 수집 기술
  - 둘 이상의 어카운트 데이터에 대한 통합 분석 설계 기술
  - 포렌식 툴로서의 증거 보존 설계 기술
- SNS 포렌식 데이터 시각화 분석 기술
  - SNS 포렌식 데이터 시각화 공통 데이터 포맷 설계 기술
  - Dynamic Graph를 이용한 시각화 분석 기술
  - Timeline을 이용한 시각화 분석 기술

2. 개발기술의 주요내용(4)

표준화 및 특허

관련 기술의 표준화 동향

- 구글, 야후, 마이스페이스 등 22개사는 오션소셜 Foundation을 구성하였고 오션소셜은 소셜 프로그램을 위한 웹 공통 API를 제공하여 하나의 프로그램을 여러 웹 사이트와 연동하는 소셜 네트워크 서비스가 가능함
- OMA 는 모바일 단말과 소셜 네트워크 서버들 사이의 통신 방법에 관한 표준화를 진행중임
- W3C의 연방형 소셜 웹 표준화는 사용자의 사생활을 보호하면서 서로 다른 소셜 네트워크 서비스를 연동하기 위한 문제점을 다루고 있음
- SNS 포렌식 데이터의 시각화에 대한 표준은 아직 없음

보유 특허

출원/ 등록 구분	특허명	출원국 (등록)	출원(등록)번호	출원(등록) 년도
출원	소셜 네트워크 포렌식 장치 및 이 장치의 SNS 데이터 분석 방법	한국	2012-0134290	2012
출원	데이터 시각화 장치 및 방법	한국	2011-0135928	2011

3. 기술적용 분야 및 기술의 시장성(1)

기술이 적용되는 제품 및 서비스

기술이 적용되는 제품/서비스

- SNS 포렌식 도구를 이용한 컴퓨터 포렌식 시스템
- 다수의 SNS 사용자들 행위들간의 상호 연관관계를 분석하기 위한 포렌식 분야
- 해킹, 회사기밀 유출, 컴퓨터 범죄 등 사이버 범죄에 대한 수사 지원 서비스
- 기업기밀 누출 방지, 회계부정 방지, 비밀 데이터 통제관리 방안에 적용
- 다양한 지적재산권 보호, 내부정보 유출 방지, 회계 감사 등 민간 서비스 분야
- 시각화 기법을 활용한 데이터 분석 분야

3. 기술적용 분야 및 기술의 시장성(2)

해당 제품/서비스 시장 규모 및 국내외 동향

해당 제품/서비스 시장 규모

- 전 세계 디지털 포렌식 관련 SW 시장은 2010년 $48억에서 연평균 11%씩 증가하여 2016년에는 $82억에 이를 것으로 추정됨
- 이전 기술과 직접적으로 연관된 SW 부분의 해외시장 규모는 2012년 $16억에서 2016 년에는 $24억에 이를 것으로 추정되며, 국내시장 규모는 2012년 981억원에서 2016년에는 1,490억원으로 증가 예상

Worldwide Legal Discovery Infrastructure Revenue by Product Segment, 2005–2013 ($M)

	2005	2006	2007	2008	2009	2010	2011	2012	2013	2008–2013 CAGR (%)
Software	2,121	2,424	3,147	3,724	3,925	4,324	4,877	5,452	6,054	10.2
Services	6,167	6,578	7,071	7,366	7,138	7,385	7,833	8,277	8,831	3.7
Hardware	1,254	1,254	1,480	1,702	1,787	1,894	2,046	2,230	2,431	7.4
Total	9,543	10,257	11,698	12,791	12,850	13,603	14,756	15,958	17,316	6.2

[Worldwide Legal Discovery Infrastructure 2009-2013 Forecast,IDC,2009
국내 시장은 IDC의 전 세계 시장 예측 규모 중 5% 점유 예측

해당 제품/서비스 시장 국내외 동향

- 시장을 선도하는 SNS 포렌식 제품은 i2 Analyst Notebook과 X1 Social Discovery이 대표적임
- 웹 기반의 본 기술과는 달리 독립 어플리케이션 형태로 존재함
- 국내 인터넷 범죄 수사센터, 사이버 테러 대응센터를 비롯한 대부분의 국가기관들은 해외에서 개발된 컴퓨터 포렌식 절차 및 기술을 사용

4. 기대효과

기술도입효과

고객이 본 기술을 통해 얻을 수 있는 경제적 효과

- 널리 사용되는 X1 Social Discovery 는 연간 라이선스를 지불하는 상용도구로서 유지 비용이 큼. 하지만, 본 기술은 데이터 수집과 분석 도구를 분리하여 저렴한 비용으로 처리 가능
- 웹 브라우저를 이용하여 다수의 분석관이 SNS 포렌식 수집 및 시각화 분석 시스템에 접근가능하기 때문에 멀티 카피의 도구 구입이 필요없음
- 본 기술의 시각화 데이터 포맷 및 시각화 모델링 방식을 다른 포렌식 분야에도 적용 가능
- 포렌식 환경 변화에 대응하는 기술 개발로 검찰, 경찰, 국방 등 국가 사법 기관의 국가 과학수사 기술력 증대
- 컴퓨터 범죄, 해킹, 회사기밀 유출 등 컴퓨터, 사이버 범죄에 대한 효율적 분석 수단 법 제공