윈도우 레지스트리 증거수집기

최규하, 신예찬, 조윤석
수원대학교 정보보호학과
e-mail:chlrbgk130@naver.com dpckstls@naver.com jys2749@naver.com

Windows Registry Digital Evidence Collector Development

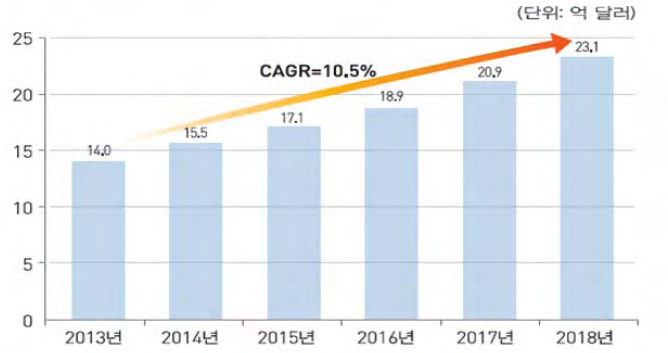
Gyu-Ha Choi, Yea-Chan Shin, Youn-Seok JO
Dept of Information Security, Suwon University

요 약

우리는 ICT의 발전과 디지털 장치의 빠른 대중화 속도에 의하여 유비쿼터스가 현실화 되고 있는 사회에 살고 있다. 그러나 빠른 속도로 기술이 발전하는 반면에 사이버 범죄의 대한 인식과 대처는 발달의 속도를 따라가지 못하고 있다. 사이버 범죄는 다양한 방법으로 늘어가고 그에 따른 피해가 커지고 있지만 일반인들은 그에 따른 대처를 하지 못하고 전문가에게만 의존하고 있다. 따라서 우리는 일반 사용자도 쉽게 사용할 수 있는 레지스트리 분석기를 개발하여 디지털 포렌식 관점에서 유용한 정보를 제공하고 개인정보 침해 및 각종 디지털 범죄에 대한 인식을 개선시켜 보려고 한다.

1. 서론

현대 사회는 ICT 발전으로 인해 언제 어디서든 다양한 정보를 쉽게 얻고 공유할 수 있게 되어 편리하고 스마트한 세상이다. 그러나 이러한 편리한 생활 속에서 크래커들로 인하여 디지털 범죄에 노출되어 개인정보 유출 및 다양한 피해가 일어나고 있다는 사실을 많은 사람들은 인지하지 못하고 있다.



위 표에서 볼 수 있듯이 디지털 범죄가 늘어나는 만큼 디지털 포렌식 시장의 규모는 꾸준하게 성장하고 있으며 관련 특허기술의 출원 또한 늘어나고 있다. 여기서 디지털 포렌식이란 검찰, 경찰 등의 수사 기관을 기준으로 정의하면 디지털 범죄 수사라고 부를 수 있으며 더 넓은 의미로는 증거수집, 증거분석, 보고까지의 수사절차 및 관련 기술을 연구하는 학문 및 응용 분야로 정의된다. 이러한 디지털 포렌식은 과정도 복잡하고 용어도 생소하여 일반인들에게 접하기 어려운 전문가의 영역이라고 느낄 수 밖에 없다. 따라서 우리는 쉽게 사용할 수 있는 윈도우 레지스트리 분석기를 개발하여 일반인이 디지털 포렌식에 대한 진입 장벽을 낮추고 관심을 가질 수 있도록 유도하여 보안의식을 확고히 하는데 조금이나마 기여 하려고 한다.

본 논문의 구성은 다음과 같다. 2장에서는 레지스트리에 대한 설명과 수집기를 개발하는데 사용한 기술들을 설명할 것이다. 3장에서는 분석기의 요구사항 및 자세한 기능을 소개하고 4장에서는 분석기의 기대효과 및 활용 분야를 서술 할 것이다. 마지막으로 5장에서는 향후과제를 소개하여 앞으로 개발할 방향성에 대해 서술하려고 한다.

2. 레지스트리 증거 수집기 설계

레지스트리는 윈도우 운영체제에서 운영체제와 응용프로그램 운영에 필요한 정보를 저장하기 위해 고안한 계층형 데이터베이스의 저장소이다. 본 장에서는 분석에 사용되는 데이터와 프로그램에 사용된 기술에 대해 서술한다.

2.1 수집 데이터

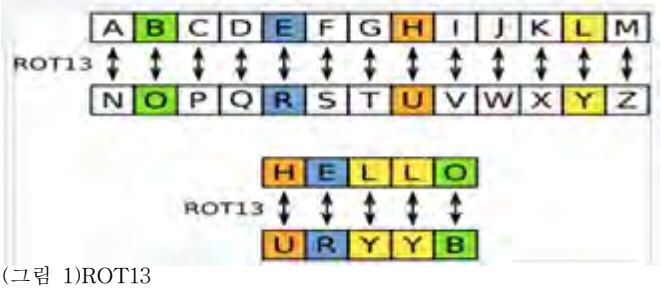
포렌식 관점에서 레지스트리 분석은 온라인 레지스트리 분석과 오프라인 레지스트리 분석으로 나뉘는데 본 프로그램에서 수집하는 데이터는 온라인 레지스트리 분석을 하며 ,이는 활성화 시스템에서의 레지스트리 분석을 의미한다. 추가적으로 RegEdit(regedit.exe)나 RegEdit32(regedit32.ex

e)을 통해 활성화 시스템에서의 레지스트리를 확인할 수 있다.

2.2 사용 기술

2.2.1 ROT13(Rotate by 13)

단순한 카이사르 암호의 일종으로 영어 알파벳을 13글자씩 밀어서 만들며, 해당 기술은 레지스트리의 응용프로그램의 VALUE값을 변경하기 위해 사용하였다.



(그림 1)ROT13

2.2.2 순차 탐색(Sequential Search)

데이터 집합의 처음부터 끝까지 차례대로 모든 요소를 비교해서 데이터를 찾는 탐색 알고리즘이며, 정렬되어 있지 않은 레지스트리 정보를 수집하기 위해 사용 하였다.

2.2.3 윈도우API(Windows API)

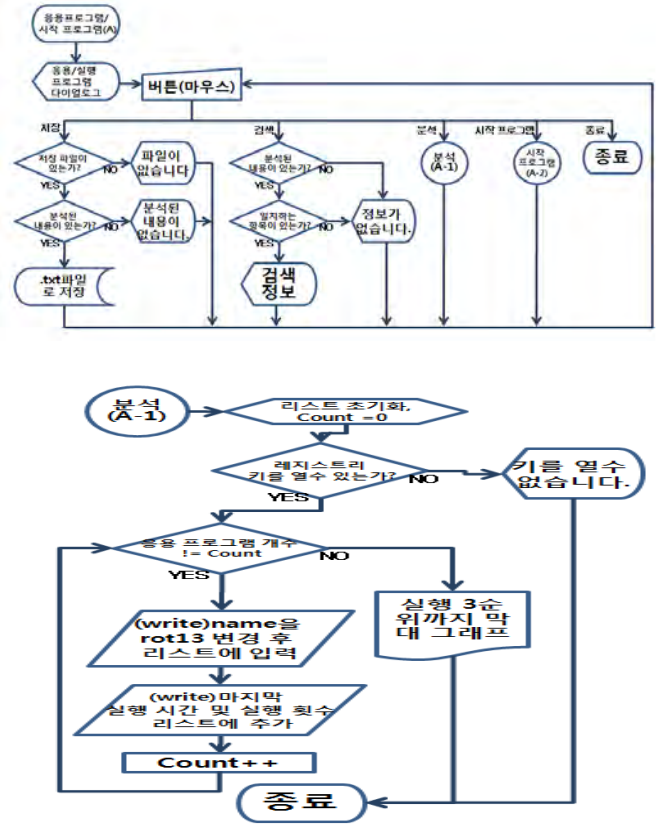
윈도우 운영 체제들이 사용하는 API이며 C/C++ 프로그램에서 직접 운영 체제와 상호 작용할 수 있도록 만들어졌으며, 이를 통해 레지스트리에 접근 할 수 있었다.

3. 레지스트리 증거 수집기 구현

C++ 기반의 MFC를 이용하여 온라인 레지스트리 데이터를 수집 및 분석하는 증거 수집기를 구현하였으며,
이 증거 수집기는 응용프로그램, 시작프로그램, 최근 사용 문서, 무선AP, USB기록을 업무 사용자가 사용할 수 있도록 수집 및 분석한 내용을 보여준다.

3.1 응용 프로그램

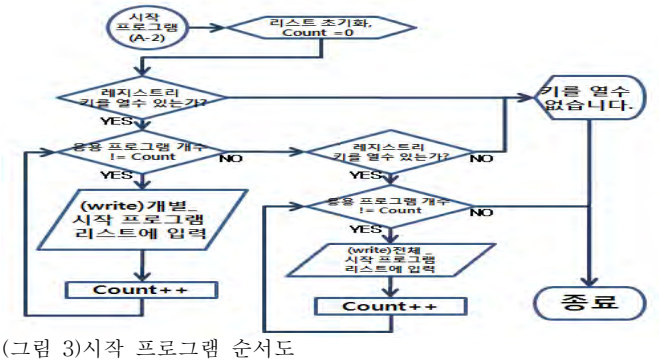
응용프로그램은 수집, 검색, 저장 기능을 구현한다. 수집기능은 응용프로그램 이름, 사용 횟수, 마지막 사용 시간 순으로 리스트에 추가한다. 그리고 이 수집된 내용으로 실행 1,2,3 순위를 막대그래프로 출력한다. 검색기능은 수집 이전에는 사용하지 못하며, 대소문자, 공백을 구분하며, 검색 후 출력되는 정보는 이름, 변경되기 전 이름, 사용 횟수, 마지막 사용시간, 데이터를 표현한다. 저장기능은 검색 기능과 같이 수집 이전에는 사용하지 못하며, 이름, 시간, 사용 횟수를 텍스트 형식으로 저장한다.



(그림 2)응용 프로그램 순서도

3.2 시작 프로그램

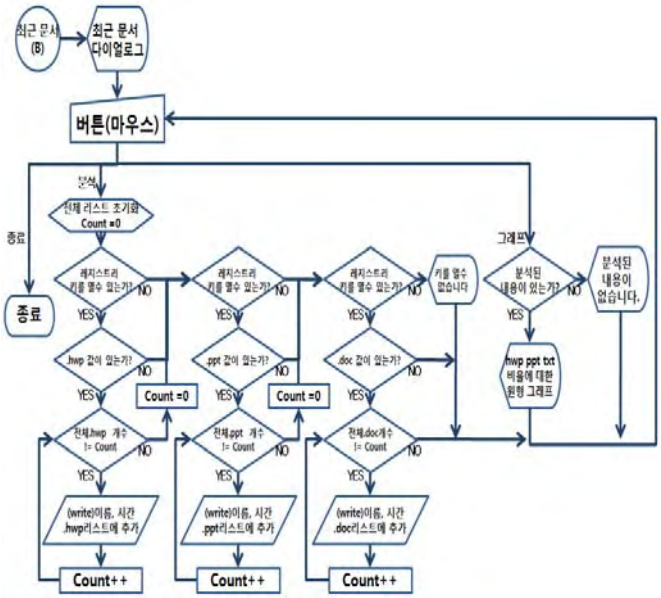
시작 프로그램은 수집, 폴더열기 기능을 구현한다. 수집기능에서는 이름, 경로 순으로 리스트에 추가하며 폴더 열기 기능은 수집 이전 사용 불가능 하며, 리스트를 선택하여 해당 파일의 폴더를 열도록 한다.



(그림 3)시작 프로그램 순서도

3.3 최근 사용 문서

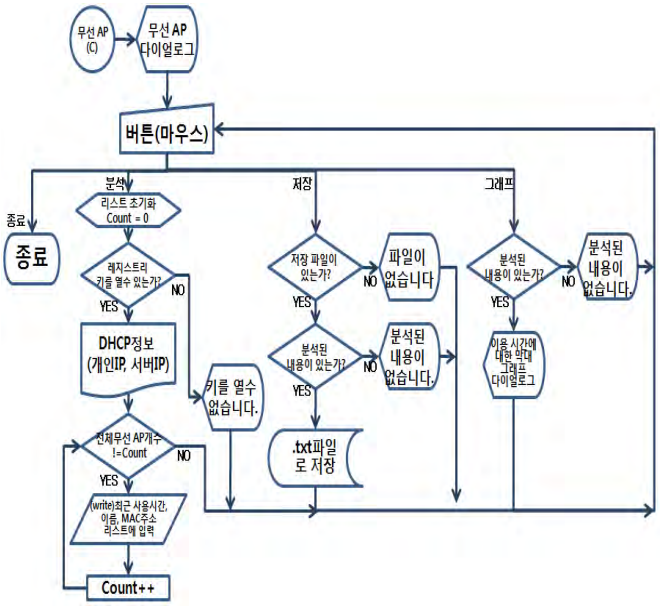
최근 사용 문서는 분석, 그래프 기능을 구현한다. 분석 기능은 3가지 확장자(.hwp, .ppt, .doc)를 최근에 수정된 시간 순서로 이름, 경로, 수정된 시간을 리스트에 추가한다. 그래프 기능은 원형 그래프로 표현하고, 3가지 확장자와 3가지 확장자를 제외한 나머지 확장자를 .etc로 표현하여 각 다른 색으로 구분한다.



(그림 4)최근 문서 순서도

3.4 무선AP

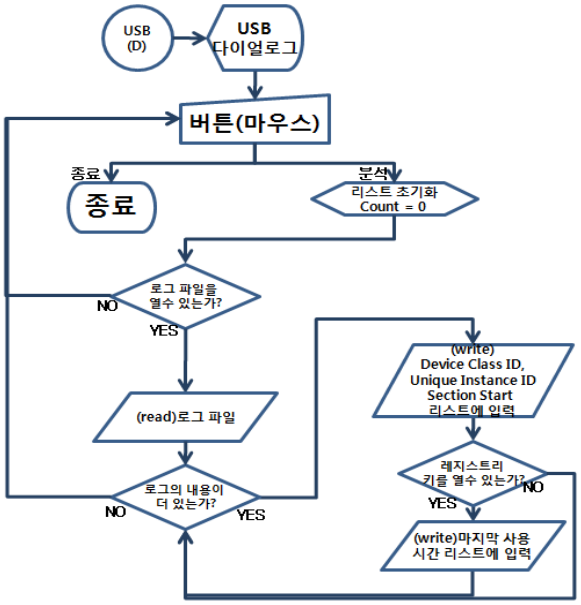
무선AP는 수집, 그래프, 저장 기능을 구현한다. 수집 기능은 무선AP 연결 기록을 최신순으로 리스트에 최근 사용 시간, 이름, MAC 주소 순서로 리스트에 추가한다. 그래프 기능은 수집된 무선 AP의 시간을 분석하여 24시간을 2시간 단위로 구분하여 시간별 사용 빈도 막대그래프를 출력한다.



(그림 5)무선 AP 순서도

3.5 USB

USB는 분석 기능이 있다. USB기록이 수집된 정보를 Device Class ID, Unique Instance ID, Section start, 최근 사용 시간 순으로 리스트에 추가한다.



(그림 6)USB 문서 순서도

4. 기대효과 및 활용분야

프로그램을 통하여 기대하는 효과는 사용자는 최근 사용한 프로그램, 최근 문서 목록과 무선 AP 연결 정보를 확인 할 수 있다. USB사용 흔적을 통하여 외부에서 어떠한 USB를 사용 했는 지 확인 할 수 있다. 프로그램의 사용이 쉽기 때문에 실무자에게는 레지스트리에서 정보를 수집하고 가공하는 수고를 덜어 주고 일반 사용자에게는 디지털 포렌식에 관심을 유도하고 보안의 중요성을 확립 시킬 수 있다.

활용분야는 사용자가 프로그램 사용 횟수, 빈도, 무선 AP 시간별 이용시간을 확인하여 사용 패턴을 알 수 있다. 침입자가 접근하였다면 어떠한 프로그램을 사용 하였는지, 언제 접근하였는지 확인하는데 유용한 정보를 제공해 준다. 또 외부에서 USB로 침입 한다면 USB기록을 통해 다른 사용자가 접근 한 기록을 확인 할 수 있다.

5. 향후과제

5.1 증거 수집기 프로그램에 개선사항

레지스트리 편집기 접근기록 및 원격 접속기록도 분석할 수 있도록 기능을 추가할 것이고 실시간으로 변경되는 데이터들을 바로 적용 할 수 있도록 구현할 것이다. 또한

직관적이고 심플한 UI를 통해 사용자들이 사용하기 쉽고 한눈에 알아볼 수 있도록 할 것이다.

레지스트리에서 얻을 수 있는 정보의 한계가 있기 때문에 이벤트 뷰어 및 로그파일을 분석하여 보다 자세하고 유용한 정보를 얻을 수 있도록 할 것이다.

참고문헌

[1] 참고문헌

임경수, 박종혁, 이상진, “디지털 포렌식 현황과 대응 방안” 보안공학연구논문지 제 5권 제 6호 2008년 12월

[2] 참고문헌

김한기, 김도원, 김종성, “레지스트리 접근권한 변조에 관한 포렌식 분석 연구”
정보보호학회논문지 26(5), 2016.10, 1131-1139 (9 pages)

“본 논문은 2017년 한이음 ICT멘토링 프로젝트의 결과물입니다.”