2008년 정보보호학과 졸업작품

Encase 이용한 사이버 범죄 수사

팀명 : 범죄의 재구성

팀 원

강정기 박광선
박진웅 이동운
이숭희 이재용
이충환 최봉겸

2008. 10

중부대학교 정보보호학과

목 차

1. 서 론 · 1

1.1 Digital Forensics · 1

1.2 Digital Forensics 필요성 및 기술 · · · · · · · · · · · · · · · · 3

2. 기반기술 · 5

2.1 Encase? · 5

2.2 증거수집 · 8

2.3 증거분석 · 11

2.4 증거제출 · 14

2.5 포렌식 시스템 및 툴 현황 · · · · · · · · · · · · · · · · · · · 14

2.6 포렌식 활용 분야 · 15

3. Encase를 이용한 Digital Forensics · · · · · · · 17

3.1 Interactively Unified Invesigation Model · · · · · · · · · · · · 17

3.2 Log 분석 시나리오 · 19

3.3 E-mail분석 · 22

3.4 USB 분석 시나리오 · 24

3.5 인터넷 History · 30

4. 결 론 · 31

5. 참고문헌 · 33

<그림 차례>

그림 1 · 4
그림 2 · 10
그림 3 · 11
그림 4 · 15
그림 5 · 17
그림 6 · 19
그림 7 · 20
그림 8 · 20
그림 9 · 21
그림 10 · 22
그림 11 · 23
그림 12 · 23
그림 13 · 24
그림 14 · 25
그림 15 · 25
그림 16 · 26
그림 17 · 26
그림 18 · 27
그림 19 · 27
그림 20 · 28
그림 21 · 28
그림 22 · 29
그림 23 · 30
그림 24 · 30

1. 서 론

1.1 Digital Forensics

정보통신 전문가들은 향후 5년간 세상을 바꿀 10대 신기술로서 유비쿼스, 컴퓨팅,초고속 인터넷, 차세대 디스플레이(OLED)이 등 IT 관련 기술을 주목하고 있다. 가정의 디지털 TV, 인텔리전트 냉장고 등 가전기기도 네트워크를 통해 유·무선으로 연결돼 외부에서 언제든지 조작이 가능하고, PDA, 이동전화, 차량에 설치된 노트북, 회사에서 사용하는 컴퓨터 등 언제 어디서나 인터넷과 컴퓨터가 연결되는 유비쿼터스 세상이 도래 할 것이다. 그러나 이러한 장점에도 불구하고 인터넷은 해킹, 정보 유출, 서비스 거부 공격 등 보안 사고에 대한 많은 취약점을 갖고 있다. 2003년 초에 발생한 ' 1.25 인터넷 대란'에서 외부 해커나 웜 등의 공격으로 인해 인터넷 기간망이 마비되는 초유의 사태를 경험을 하였다. 이러한 침해 사고는 우리 사회에 큰 파장을 불러 왔다. PC방, 게임 업체, 인터넷 쇼핑몰 등 온라인을 이용하여 업무를 수행하는 회사에서는 큰 손실을 보았고, 전자 상거래나 인터넷 뱅킹 등에 대한 불신도 가중 되었다. 또한 해커 수준의 전문 지식이 없어도 약간의 노력만으로 개인 정보 유출이 가능하며 이로 인한 피해는 심히 우려되는 상황에 이르렀다. 더욱 다양한 형태로 확산되고 있는 침해 사고는 특정 개인이나 기업만의 문제에 그치지 않고 사회의 질서를 파괴하는 범죄로서 인식되고 있다. (Gordon, et al., 2004; Stephenson, 2004) 또한 이러한 사고 발생시 이에 대한 법적 증거 자료 수집에 대한 방법과 증거 수집이 어렵다는 단점을 가진다. 그렇기 때문에 요즘 대두화 하는 디지털 포렌식은 해킹이나 개인 정보 유출시 "법정의", "공개토론이나 변론에 사용되는","수사와 법정에서의 증거 또는 사실 관계를 확정하기 위하여 사용하는 과학이나 기술에 관한 (Houghton Mifflin Company, 200)", "범죄와 관련된 증거물을 과학적으로 조사하여 정보를 찾아내기 위한 (Combridge University Press, 2006")이라는 의미를 갖는다. 포렌식은범죄와 관련된 분야에서 Forensic Examination, Forensic Laboratory, Forensic Medicine, Forensic Science 등의 용어로 사용되어 왔으며, 최근에는 범죄수사 및 민 ·형사소송 등 법정에 사용되는 증거의 수집, 보존, 분석을 위한 응용과학 분야를 통히는 용어(최득신, 2006;Herath, et al,2005 : 135-141)로 사용되고 있다.

전통적으로 포렌식은 법의학 분야에서 지문, 모발, DNA 감식, 변사체 검시 등이주류를 이루었다. 얼마전 사회적 이슈가 되었던 줄기세포 조작사건의 경우에도 DNA감식이 수사에 중요한 역할을 담당 하였다. 그러나 최근 다양한 정보기기들의 활용과 정보생산 및 유통에 있어서 95% 이상이 디지털 형태로 이루고 있기 때문에 물리적 형태의 증거뿐만 아니라 적자적 증거(Electromic evidence)를 다루는 디지털 포렌식(Digital Forensics) 분야가 점차 확대되고 있다. 하드웨어, 소프트웨어, 또는 컴퓨터 내의 데이터를 불법적으로 사용하거나 변경, 파괴하는 행위를 컴퓨터 범죄라고 한다. 이러한 컴퓨터 범죄에 대한 수사는 전자적 신호를 전송되거나 저장 매체에 기록되는 전자적 증거를 수집하고 분석하기 위한 지식과 기술을 요구한다. 수사의 근본적인 특성에 따라 법적으로 유효한 전자적 증거의 확보를 목표로 과학적 지식과 기술을 활용하여 전자적 증거를 수집하고 분석하는 제반 행위를 디지털 포렌식이라고 한다.

미국에서는 90년대 이후 아동 포르노, 해킹, 개인정보 유출, 기술 유출 등 컴퓨터 범죄의 위협이 증가하면서 디지털 포렌식의 연구·개발을 위한 연구실과 민관 교육기관이 설립되고 관련 교육과정이 개설되기 시작 하였다. 디지털 포렌식이라는 용어도 1991년 포렌식 교육을 목적으로 한 법집행기관의 전문가들이 결성한 비영리 단체인 국제 컴퓨터 수사 전문가 협회(IACIS)가 미국 포틀랜드에서 개설한 교육과정에서 처음으로 사용되었다.
디지털 증거에 대한 과학적인 조사를 주요 내용으로 하는 디지털 포렌식은 탐정 제도 등이 발되 어 있고 적법 절차를 중히사는 영·미 등 선진국에서 많이 발전되어 왔으며, 민·형사 소송의 증거에 매우 중요한 역할을 해왔다. 디지털 포렌식은 컴퓨터를 이용한 수사 혹은 컴퓨터와 관련된 수사과정에서 과학적이고 체계적인 증거 확보 절차에 따라 합법적인 증거를 산출 해냄으로써 정확한 범죄자 색출 및 범죄 사실의 증명을 통한 실체적 진실의 발견에 크게 기여할 수 있다. (Winlsdion, et al., 2005: 48-55)

유비 쿼터스 컴퓨팅 등 새로운 패러다임을 선도하는 정보사에서 범죄 증거는 다양한 형태로 존재하게 되고 디지털 포렌식 기술은 더욱 중요하게 될 것이다. 그러나 국내에서는 수사기관이나 일부 보안 업체를 중심으로 최근 디지털 포렌식에 대한 관심이 급증 하였다. 향후 디지털 포렌식에 대한 관심과 연구를 활성화 하여 압수수색 및 분석 분야에 우선 적용하면서 표준 절차를 개발하고, 이러한 절차를 통해 얻어낸 증거가 형사 사법의 이념인 실체적 진실의 발견 과 적법 절차 원칙 실현에 중요한 역할을 하여야 하며, 또한 피의자의 인권 보호에도 기여 하여야 할 것이다.

1.2 Digital Forensics 필요성 및 기술

컴퓨터와 인터넷은 인간의 생활을 놀라울 정도로 변화시켜 왔다. 특히 우리나라는 초고속 인터넷 보급률리 세계 1, 2위를 다룰 정도로 정보화에 앞선 국가로 실제 생활에서 이루어지는 대부분의 것들이 사이버공간에서 이루어질 정도이다. 하지만 그에 대한 부작용도 만만치 않아서 과거에는 없었던 인터넷을 대상으로 한 새로운 범죄행위들이 끊임없이 등장하고 있으며, 설상가상으로 정보보호에 대한 투자가 미흡한 국내 현실로 인해 사이버 범죄자들의 주된 활동무대가 되고 있는 안타까운 실정이다.
사이버 범죄의 경우 범죄가 발생하는 영역이 지역적이지 않고 범죄의 증거가 원격지에 존재하는 경우가 많으므로 사이버 범죄에 대한 증거를 분석하기 위해서는 국제 공조가 필수적이라 할 수 있겠다. 또한 범죄에 대한 단서가 대부분 디지털 형태로 저장되어 있는 특성으로 인해 삭제, 변경 등에 취약한 디지털 데이터에서 법적 증거력있는 디지털 증거를 추출하기 위해서는 전문적이고 논리적인 절차와 방법을 따라야 한다. 이러한 일련의 과정과 원칙 등을 포괄하여 디지털 포렌식이라 한다. 디지털 포렌식은 비단 사이버 범죄의 증거를 획득하기 위해서만 적용되는 것이 아니라, 일반 범죄의 경우에도 범죄의 증거자료가 개인 PC의 하드디스크 등에 저장되어 있다면 그 증거를 찾아내기 위해 하드디스크를 분석하는 과정에 적용되어야 한다.

□ Digital Forensics 기술

디지털 증거 획들을 위한 데이터 처리는 평가, 수집, 조사 및 문서화와 보고의 4단계로 이루어진다. 이는 범죄 현장에서 범죄에 사용되었거나 연관된 디지털 증거를 포함하고 있는 시스템을 가려낸 후, 해당 시스템으로부터 디지털 데이터를 수집하고, 수집된 데이터를 이용해 디지털 증거를 추출하는 조사과정을 거친 후 디지털 증거 및 조사과정을 문서화하여 보고하는 일련의 과정을 포함한다. 디지털 포렌식 도구는 위에서 정의한 각 과정을 독립적으로 수행할 수도 있고, 전체 과정을 포함하는 하나의 통합 시스템 형태로 존재할 수도 있다.

전체 포렌식 도구에 필요한 요소기술을 정의하면 크게 원본 데이터로부터 데이터를 수집하는 기술과 디지털 데이터를 분석하여 증거를 추출하는 기술로 나뉠 수 있다. 원본 데이터로부터 데이터를 수집하는 기술은 저장매체 이미징 기술, 이미지 인식 기술, 디지털 증거 무결성 확보 기술, 활성 시스템 정보수집 기술 및 네트워크 정보수집 기술이 있다. 원본 데이터는 개인 PC의 하드디스크 등 일반적인 디지털 저장매체에 존재할 수도 있고, 활성 상태인 시스템의 메모리가 그 대상이 될 수도 있으며 네트워크 상에 전송 중인 데이터가 수집 대상이 될 수도 있다. 어떤 경우이든 [그림 1]와 같이 원본을 보존하기 위해 원본과 동일한 사본을 생성한 후 사본을 대상으로 디지털 증거를 추출하는 것을 원칙으로 하므로 이미징 기술 및 이미지 인식 기술이 필수적이고, 수집한 디지털 데이터에 대한 무결성 확보 기술이 추가적으로 요구된다.

[그림 1] 디지털 데이터 수집

디지털 데이터로부터 디지털 증거를 추출하기 위해서는 데이터 고속 검색/분석 기술, 삭제/손상 데이터 복구 기술, 패스워드 검색 및 암호해독 기술, 정보은닉 탐색 및 추출 기술, 네트워크 분석 및 역추적 기술 등이 요구된다. 범죄의 증거는 악의적인 목적으로 삭제되거나 손상된 데이터를 복구할 수 있어야 하고, 증거가 될 수 있는 파일에 대한 함호해독이 가능해야 한다. 또한 고도의 기술을 가진 범죄자의 경우 스테가노그래피 및 워터마킹 등을 이용해 증거를 은닉할 수 있으므로 이에 대한 정확한 탐지 기능도 추가되어야 할 것이다. 그리고 사이버 범죄에 대한 증거 추출을 위해 네트워크 분석 및 역추적 기숙이 제공되어야 한다.

2. 기반기술

2.1 Encase?

□ 컴퓨터 관련 범죄 증가 증거 자료의 디지털화 및 증거 자료의 디지털화

- 정보화에 따른 컴퓨터 관련 범죄뿐만 아니라 일반범죄 에서도 중요한 증거 또는 단서가 컴퓨터를 포함한 전자 매체 내에 보관되어 있는 경우가 기하 급수적으로 증가
- 디지털 자료는 복사가 쉬울 뿐만 아니라 원본과 복사본의 구분이 어렵고 조작 및 생성, 전송, 삭제가 매우 용이함.
- 범죄 관련 증거 자료가 디지털화 되어 감에 따라 증거 수집, 분석을 위한 전문적인 디지털 포렌식 기술 개발이 시급.

□ 디지털 포렌식 기술의 활용도 증가

- 국가기관에서 컴퓨터 범죄 뿐만 아니라 일반 범죄 수사에서의 활용빈도증가

- 일반기업체 및 금융 회사 등의 민간 분야에서도 디지털 포렌식 기술의 수요가 폭발적으로 증가
  - 보험사기 및 인터넷 뱅킹 피해보상에 대한 법적 증거 자료 수집 및 관리 활용
  - 내부 정보 유출방지, 회계 감사 등의 내부보안 강화 및 유지에 활용

- E - Discover 시행으로 민간 포렌식 서비스 수요 확대
  - 미국, 2006. 12. 1. 발표, SOX 나 HIPPA에 대한 세부 법 조항 시작
  - 민형사 소송에서 디지털 증거 제출 의무화
  - 매출 10억불 이상의 미국 기업들은 연평균 140여 건의 소송이 발생

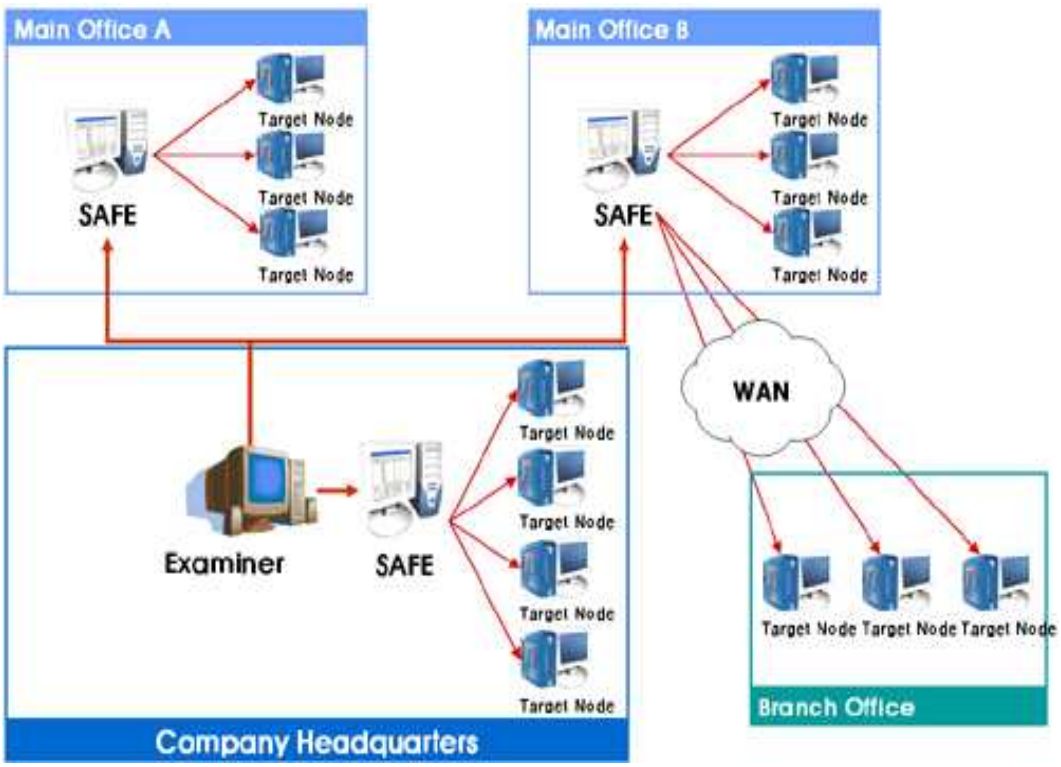
- 국내 기업의 글러벌화 및 국제화에 따른 디지털 포렌식 분야 기술 개발의 필요성 증대
  - 국내 기업의 글로벌 화 및 미국의 법과 제도를 WTO, ISO 등을 통해 국제화 하려는 추세를 감안 할 때 포렌식 분야 기술 개발 및 적용은 국내 기업의 경영 리스크를 줄이고 경쟁력 향삭을 가져옴

□ 솔루션 주요 기능

- 운본 디스크의 고속 복사 및 사본 작성 기능, 데이터 복구 기능
- 증거를 최초 발견 상태로 증거 자료 획득 및 자료 탐색 가능
- 각종 운영체계에 대한 로그의 통합관린 / 분석 및 사용자 패턴 분석
- Bit-Steaming 방식의 사본 작성 및 64K 블록마다 CRC 체크와 MD5 값 생성
- 최신 검색 엔진으로 하나의 키워드 검색 시간과 복수개의 키워드 검색 시간 동일
- 전자우판(PST, DBX) 복구를 통한 증거 수집
- 다국어 지원 (유니코드 및 한글 지원)
- 동적 디스크 지원 (Spanned, Mirrored, Striped, Raid5, Basic)

- 검색 과 분석 (키워드, 해쉬, 서명 분석, 필터)
- 북마크 와 발견물 관리 자세한 보고서 작성 기능
- 매크로
- 프로그래밍 언어인 인스크립트 기능(서치 자동화)
- 갤러리 뷰(이미지 파일 미리 보기)
- 패턴 분석 기능(TimeLine View)
- 암호 복호화 가능(EDS 추가시), IE, EFS, Outlock 등
- 휴지통 인덱스 파일 INF02 Table 검색 기능
- 파일 검색기(특정한 영역에서 특정 파일을 로드 합니다.)
- 단일 전자 우편 , IP, 주민번호, 카드번호 등 추출 가능
- 익스플로러 히스토리 분석 가능
- 바로 가기 파일 분석 기능
- 리눅스 Syslog 분석 기능
- 파티션 파인터(고급 데이터 복구 기능)
- 윈도우 이벤트 로그 분석 기능
- 라이브 포렌식, 원격 데이터 복구 기능 (네트워크 기능 추가시)
- 용의자의 환경으로 즉시 부팅하여 조사 가능(PDE 추가시)
- SCSI, USB、 E-IDE Devce 사본 작성 가능 (무결성 보장)
- FAT12 FAT16, FAT32, NTFS, HFS, HFS+, UFS, Solaris, AIX, JFS, JFS2, Ext2/3, Reiser, Pal, CDFS, Jolie, UDF, 지원 가능

□ 구성 및 구성 주요 기능



- SAFE (Secure Authentication For Encase, 필수 요소)
  • PKI 인증, Examiner 접근 제어, 사용자 생성, 역할 지정, 보안 로그인을 제공하여 타겟 시스템에 비트 - 레벨로 접근 할 수 있는 사용자를 관제하고 통제 가능.

- Examiner (필수요소)
  • SAFE로 로그인하여 권한고 k역할을 확인 받은 후 대상 네트워크 노드로 포렌식 업무와 조사를 진행 가능.

- Servlet (on Target, Nodes, 필수 요소)
  • 네트워크 노드에서 실행되는 서블릿(클라이언트)은 자동으로 실행할 수 있고 원격으로 자동화 설치가 가능.
  • 현재 윈도우, 리눅스, 솔라리스, AIX, OSX 지원
  • The servlet (on Target Nodes)

- PDE Module (Physical Disk Emulator, 옵션 요소)
  • 포렌식 업무에서 용의자의 OS 환경으로 부팅하여 조사하는 것은 필수
  • PDE 모듈과 VMwaer 의 조합은 인케이스, DD, Safe Back등의 증거 파일을 가지고 즉시 용의자의 OS 환경으로 부팅하여 안전하게(쓰기작업 없이, 디스크 복원 없이) 과학 적인 수사를 가능케 함

- VFS Module (virtual Fole System, 옵션 요소)
  • Encase, DD, SafeBack 등의 증거 파일을 읽기 전용 네트워크 드라이브로 마운트하여 윈도우 익스플로러가 접근할 수 있게 함.
  • 미디어에 바이러스 검사를 수행하여 Rootkit 이나 트로이잔을 검출하고 조사자가 가지고 있지 않은 많은 응용 프로그램을 실행할 수 있게 함.

- EDS MNodule (Encase Decryption Suite, 옵션 요소)
  • 한국으로 수출이 제한되어 있으나 2005년부터 제품 공급이 가능
  • 윈도우2K/XP등의 OS에서 “ 폴더 암호화” 수행으로 EFS가 설정된 경우 EFS 복호화를 성공적으로 수행할 수 있는 전 세계적인 유일한 툴.
  • 인터넷 익스플로러 등에서 자동으로 입력된 암호를 추출 및 Outlook2k3등의 함호를 복호화 할 수 있음.

2.2 증거수집

보통의 디지털 기기는 운영체제가 탑재되어 있으며, 운영체제는 휘발성 저장매체와 비휘발성 저장매체를 사용한다. 휘발성 저장매체란 DRAM과 같이 컴퓨터 운영체제가 종료되면 더 이상 데이터를 복구 할 수 없는 저장매체를 말하며, 비휘발성 저장매체란 EEPROM, 플래시메모리, 하드디스크와 같이 운영체제가 종료된 이후에도 데이터를 복구할 수 있는 정장매체를 말한다. 디지털 포렌식에서 증거 수집은 대상 매체의 운영체제 종료 여부에 따라서 다음과 같이 나눌 수 있다.

- 데드 시스템상에서의 증거 수집 : 운영체제가 종료된 컴퓨터나 핸드폰 같은 기기에 대한 증거 수집을 말하며, 주로 하드디스크나 플래시 메모리로부터 데이터를 얻는 것으로 이루어진다.
- 라이브 시스템상에서의 증거수집 : 운영체제가 종료되지 않는 컴퓨터나 핸드폰 같은 기기에 대한 증거 수집을 말한다. 하드디스크와 같은 비휘발성 매체뿐만 아니라 컴퓨터 메모리와 같은 휘발성 저장매체로부터 데이터를 얻는 것으로 이루어진다.

라이브 시스템상에서의 디지털 포렌식을 수행하기 위해서는 운영체제가 사용중인 휘발성 메모리와 하드디스크를 접근할 필요가 있다. 하지만 Windows와 같은 운영체제에서는 중요한 메모리 영역이나 하드디스크상의 파일에 대한 사용자 프로그램의 접근을 막고 있다. 따라서 라이브 시스템상에서의 포렌식을 위해서는 운영체제의 보호기능을 우회 할 수 있는 기술이 필요하다.

□ 데드 시스템상에서의 증거 수집

데드 시스템상에서의 증거 수집 기술은 포렌식 대상 기기에 따라 달라지게된다. 핸드폰 기기와 같이 비휘발성 저장매체를 분리 및 접근하기가 용이하지 않은 기기는 상대적으로 컴퓨터 하드디스크와 같이 쉽게 저장매체를 분리 및 접근할 수 잇는 기기보다 데이터 획득이 어렵다. 데이터를 쉽게 획득할 수 있는 컴퓨터 하드디스크에서도 원본 데이터의 이미지를 만들게 되는데, 이는 나중에 증거분석을 할 경우에 원본데이터가 변경되는 것을 막기 위해서이다. 따라서 본 저장매체에 잇는 데이터의 무결성을 보장 할 수 있는 이미징 기술이 필요하다.

□ 라이브 시스템상에서의 증거 수집

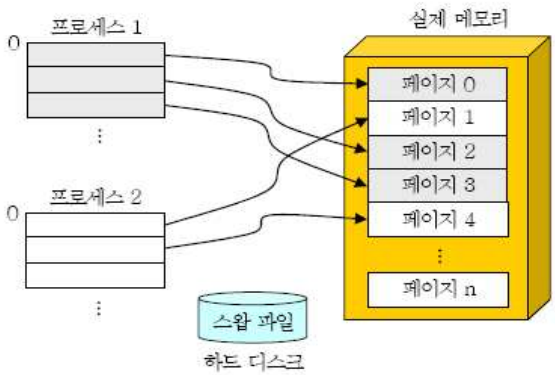
운영체제가 종료되지 않은 시스템에서의 데이터 획득 순서는 휘발성 저장매체있는 데이터들을 먼저 획득한 후에, 비휘발성 저장매체에 잇는 데이터들을 획득 하는 순서로 이루어진다. 포렌식 대상이되는 라이브 시스템에서 휘발성 저장매체나 비휘발성 저장 매체에서 데이터를 획득하기 위해서는 라이브 시스템 운영체제에 잇는 명령어들을 사용하기 보다는 포렌식 툴을 사용해서 데이터를 획득해야 하는데, 그 이유는 다름과 같다.
첫째, 대상 시스템의 운영체제 명령들이 공격자에 의해서 이미 바뀌어 있어서 그 명령을 사용할 경우 사건 증거들을 삭제할 가능성이 있기 때문이다.
둘째, 운영체제 명령어들이 바뀌지 않았다 하더라도, 정상적인 운영체제 명령의 실행이 시스템 정보를 변경할 가능성이 있기 때문이다. 예를 들어 보면, Windows운영체제에서 단순히 탐색기 창을 여는 것만으로 여러 파일들의 마지막 접근 시간(accessed time)이 변경되게 된다. 파일과 관련해서 여러 시간 정보가 존재하는데 마지막 접근 시간 이외에 마지막 수정시간(modified time), 생성시간(created time)이 존재한다.
이런 MAC(Modified Accessed,Created) 시간은 사건을 조사하는데 있어서 중요한 요소이므로 절대 변경되어 서는 안된다.

셋째, 운영체제는 시스템 보호를 위해서 일부 데이터나 파일들에 대해 사용자들의 접근을 막고 있다. 즉, 운영체제에서 제공하는 명령어들에 의해서는 접근할 수 없는 데이터나 파일들이 존재한다. 따라서 운영체제의 보호 메커니즘을우회할 수 있는 포렌식 툴의 사용이 필요하다. 라이브 시스템에서 휘발성 데이터의 획득과 비휘발성 데이터를 획득하는 데는 다양한 어려움들이 존재하며, 이는 라이브 시스템 운영체제에 따라 달라지게 된다. 다음 두 하위 절에서는 Windows나 Unix 운영체제를 사용하는 라이브 시스템에서 디지털 포렌식이 이루어지는 방식과 문제점에 대해서 설명한다.

- 라이브 시스템 메모리 덤프

Windows나 Unix 운영체제를 사용하는 시스템에서는 애플리케이션에 따라서 사용자의 ID나 패스워드가 휘발성 저장매체인 컴퓨터 메모리에 올라와 있을 수 있다. 때문에 메모리상의 데이터를 모두 얻을 수 있다면 이런 메모리 데이터로부터 중요한 정보를 획득할 수가 있다.

Windows나 Unix에서 물리적 메모리의 한계를 극복하기 위하여 [그림 1]과 같은 가상 메모리(virtual memory)를 사용하고 있다 [3],[4].



(그림 1) 가상 메모리 구조

예를 들어서, 컴퓨터의 실제 물리적 메모리는 256M 바이트라도 가상 메모리를 사용하면 각각의 프로세스는 혼자서 4G 바이트의 메모리를 사용한다고 느낄 수 있다. 이런 가상 메모리 관리를 해주는 모듈을 가상 메모리 매니저(virtual memory manager)라고 한다. 가상 메모리 매니저는 여러 프로세서의 수행을 위해서 물리적 메모리를 페이지라는 단위로 나누고 프로세스 실행시 필요한 프로세스들의 일부분을 물리적 메모리로 올려서 실행시키며, 나머지 부분은 하드디스크에 존재하는 스왑파일(swap file)에 저장시키다.

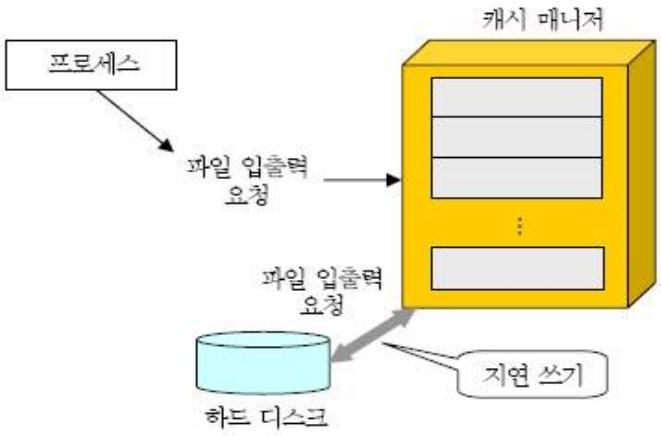
가상메모리를 사용하는 시스템에서 하나의 사용자 프로세스가 사용하는 가상 메모리를 모두 덤프하는 것은 가능하며, 덤프하기 위해서는 물리적 메모리에 있는 프로세스에 할당된 페이지뿐만 아니라 하드디스크에 있는 스왑파일 내용 일부까지 덤프해야함을 알 수 있다.

물리적 메모리의 일부분은 운영체제에 의해서 보호되고 있기 때문에 컴퓨터 부팅 전에 특별한 셋팅을 미리 해놓지 않는 한 물리적 메모리의 전부를 덤프하는 방법은 현재까지 알려져 있지 않다.

- 라이브 시스템 하드디스크 이미징

애플리케이션이나 운영체제는 중요한 데이터를 저장하기 위해서 임시 파일을 하드디스크에 만들어 사용하다가 시스템 종료 시에 삭제하는 경우가 있다. 따라서 컴퓨터를 끄기 전에 하드디스크를 이미징한다면 이런 중요한 데이터를 얻을 수 잇을 것이다. 하지만 만약 운영체제가 캐시(cache)를 사용한다면, 하드디스크만을 이미징하는 것은 데이터의 일관성(consistency)에 문제가 생길 수 있다.

파일에 대한 입출력을 좀 더 효율적으로 하기 위해서 운영체제는 (그림 2)와 같은 캐시를 사용한다. [3],[4].



(그림 2) 캐시 구조

예를 들어, 프로세스가 어떤 파일의 한 바이트를 읽어오라는 명령을 하면, 운영체제는 연속된 256K 바이트를 한꺼번에 읽어와서 캐시 메모리에 저장하고 프로세스에게는 한 바이트만을 돌려준다. 프로세스가 읽어들인 한 바이트 옆의 또 한 바이트를 읽어오라고 명령하면, 운영체제는 이번에는 하드디스크에 접근할 필요 없이 캐시 메모리에 저장된 한 바이트를 돌려주면 된다. 하드디스크 접근 시간 보다 캐시 메모리 접근 시간이 훨씬 빠르기 때문에 캐시를 사용해서 하드디스크 접근을 줄이면 시스템의 효율성이 더욱 증가하게 된다. 캐시 메모리 관리를 하는 모듈을 캐시 매니저(cache manager)라고 한다. 파일을 불러들이는 경우에는 일관성에 아무 문제가 발생하지 않는다. 일관성에 문제가 발생하는 경우는 캐시 매니저가 시스템 효율성을 높이기 위해서 지연쓰기(delayed write)를 하는 경우이다. 지연쓰기란 프로세스가 읽어들인 바이트를 수정해서 다시 파일로 쓰로도록 명령을 내릴 경우에 캐시 매니저가 캐시 메모리 데이터를 먼저 수정하고 시간이 흐른후에 하드디스크 파일에 수정된 데이터를 쓰는 것을 말한다. 지연쓰기 역시 하드디스크 접근을 줄이고 시스템 효율성을 높이기 위해서 사용된다. 지연쓰기를 하는 시스템에서 하드디스크 이미징을 하는 경우에 아직 완전히 수정이 안된 파일이 존재할 수 있으므로 일관성에 문제가 발생할 수 있다. 그러므로 하드디스크 이미징을 하기 전에 캐시 메모리에 존재하는 데이터 중에 아직 하드디스크에 기록이 안된 데이터를 하드디스크에 쓰도록 하는 기법이 필요하다.

2.3 증거분석

증거 수집에서 얻어진 데이터들로부터 유용한 정보를 얻는 것을 증거 분석이라고 한다. 유용한 정보는 사건에 따라 다르겠지만 일반적으로 다음과 같은 증거 분석 기술들이 사용될 수 있다.

□ 덤프 메모리 분석

프로세스가 사용중인 가상 메모리의 덤프를 획득했을 경우에 사용자 ID나 패스워드와 같은 유용한 정보가 가상 메모리에 남아 있을 수 있다. 프로세스를 위한 가상 메모리는 보통 코드 영역, 데이터 영역, 스택 영역 등으로 나뉘어지며, 데이터 영역이나 스택 영역이 프로세스에서 필요한 여러 정보를 저장하고 있으므로 포렌식 툴은 프로세스가 가상 메모리를 어떻게 사용하는지를 분석할 수 있어야 한다.

□ Windows 레지스트리 분석

Windows는 레지스트리(registry)에 프로그램이나 시스템에 관한 다양한 정보를 저장하고 있으므로 포렌식 툴은 이른 분석할 수 잇어야 한다. 레지스트리 HIVE 파일들은 [SystemRoot]\System32\Config폴더에 위치하며, regedit와 같은 명령으로 살펴볼 수 있다. 레지스트리 Hive 파일들 중 SAM 파일은 패스워드들의 해시 정보를 가지고 있으며, 운영체제에 의해서 암호화되어 보호되고 잇다. 포렌식 툴은 SAM 파일의 패스워드들을 복구할 수 있어야한다.

□ Timeline 분석

파일 시스템들은 각각의 파일들이 만들어진 시간정보와 마지막으로 접근된 시간 정보 그리고 마지막으로 수정된 시간 정보들을 가지고 잇다. 포렌식 툴이 이런 시간 정보를 가지고서 시간의 흐름에 따라 어떤 파일들이 생성되고 접근되었는지를 알기 쉽게 보여줄 수 잇다면 증거 분석을 좀 더 수월하게 할 수 있다. 또한 NTFS 파일 시스템에서는 $LogFile과 $UsrJrnl이라는 시스템에 대한 사용 로그를 남기고 있으므로 이로부터 좀 더 많은 정보를 얻을 수 있다.

□ 삭제된 파일 복구

하나의 파일은 여러 클러스터들의 리스트로 이루어져 있으며, 이런 리스트 정보가 파일 시스템에 들어 있다. 일반적으로 하나의 파일을 삭제할 경우에 파일시스템은 클러스터들에 들어 잇는 파일 내용을 지우는 것이 아니라 파일에 할당된 클러스터들을 프리시키는 것으로 파일을 지운다. 따라서 프리된 클러스터들이 다른 파일에 할당되지 않는 한 삭제된 파일을 복구할 가능성이 있다.
비록 삭제된 파일을 복구할 수 없을지라도 파일이 존재했다라는 사실이 사건에 중요한 단서가 될 수 있다. 어떤 파일이 존재했었는지의 존재 여부는 다양한 방법으로 이루어질 수 잇다. 예를 들어서 Thumbs.유라는 숨김 속성 파일은 디렉토리에 이미지 파일이 있을 경우에 Windows에서 이미지 파일의 정보 값을 파악하기 용이하도록 자동으로 생성하는 데이터베이스 파일이며, 이미지들을 모두 삭제해도 이 데이터베이스 파일이 남아 있을 수 있으므로 삭제된 이미지 파일의 존재여부를 증명해 줄 수 있다.

□ 비정상적인 파일 찾기

사용자가 중요한 데이터를 숨길 경우에 windows에서 파일을 숨김 속성으로 놓거나 파일 확장자를 바꾸어서 데이터를 숨기려 할 수 있다. 따라서 포렌식 툴이 숨김 속성을 가진 파일들이나 파일 확장자가 바뀐파일들을 따로 찾아줄 수 있다면 분석에 많은 도움이 될 수 있다.

보통 하나의 파일 형식은 하나의 파일 확장자를 가지며 또한 하나의 식별자(identifier)라 불리는 유일한 값을 가진다. 이 식별자는 파일 생성시 헤더에 자동으로 저장된다. 따라서 확장자를 바꿀 경우에는 파일 확장자와 이식별자가 맞니 않으므로 확장자가 바뀐 파일들을 찾을 수 있다.

□ 이메일 분석

파일 시스템에서 삭제된 파일을 복구하는 것과 비슷하게 삭제된 이메일을 복구할 수 있다. 하나의 이메일을 삭제할 경우에 이메일 프로그램은 메일박스에 있는 이메일의 내용을 지우는 것이 아니라 이메일의 헤더 값을 바꾸어서 이메일을 삭제하게 된다. EK라서 삭제된 이메일을 복구할 가능성이 있다.

□ 로그 분석

어떤 장치나 응용 프로그램을 사용하게 되면, 운영체제나 응용 프로그램이 로그를 남기는 경우가 있으며 이런 로그는 사건 분석에 중요한 정보가 될 수 있다. 중요한 로그들로는 다음과 같은 것들이 있다.

- 파일 시스템 로그: NTFS 파일 시스템의 경우 $LogFile, $UsrJrnl에 파일 생성, 접근 등에 관한 로그가 남아 있다[5].
- USB 사용 로그: USB 포트에 연결했던 USB들의 사용로그가 레지스트리에 남아 있다.
- 인터넷 사용: 임시파일, 쿠키, 즐겨찾기, ActiveX등으로부터 인터넷 사용 행적을 조사할 수 있다.

□ 슬랙 공간 분석

파일 시스템은 하나의 큰 파일을 저장할 때 여러 클러스터들로 나누어 저장하게 된다. 이 때 가장 마지막 클러스터에는 파일의 가장 뒷부분을 저장한다음 남게 되는 공간이 생길 수 있는데 이런 공간을 파일 슬랙 공간(slack space)이라고 한다. 예를 들면, 클러스터의 크기가 8K이고 파일의 크기가 1K이면, 7K의 사용하지 않는 파일 슬랙 공간이 생기게 된다. 이외에도 하드디스크에는 할당되지 않는 공간들과 볼륨 슬랙 공간, 파티션 슬랙 공간 등이 있다. 사용자들이 이런 슬랙 공간에 데이터를 숨겨 놓을 수 있기 때문에 포렌식 툴은 이런 슬랙 공간의 데이터를 분석할 수 있는 기능을 가져야 한다.

□ 스트링 서치

디지털 증거 분석시 수사에 필요한 정보가 어떤 파일에 어떤 형태로 저장되어 있는지 모르는 경우가 많기 때문에 모든 파일들을 대상으로 키워드를

가지고 검색을 반복해야 하는 경우가 많다. 이러한 검색은 대용량의 저장 매체일 경우 상당한 시간이 소요 되므로 검색범위를 축소하는 기술이 필요하게 된다. 조사 대상의 검색범위를 축소하기 위해서는 잘 알려진 파일을 검색 대상에서 제외하고, 주목해서 검색할 대상을 선정하여 검색 범위를 축소하고, 조사우선순위를 부여해야 한다. 이러한 기능을 제공하는 검색 기술 중 하나가 해시 검색(hashed serch)으로써, 준비된 참조 데이터 셋(RDS)을 사용해서 널리 알려진 파일을 조사 분석 대상에서 제외시킨다. 미국에서는 이러한 해시 검색 기술을 활성화하고, 일반 수사관들도 쉽게 사용할 수 있게 하기 위해서 잘 알려진 파일들의 표준 해시 DB를 NIST에서 제작하여 무상으로 배포하는 NSRL 프로젝트를 실시하고있다.[6] NSRL 프로젝트 목적은 "범죄에 사용되는 컴퓨터 파일의 식별 자동화", "증거에 포함된 파일조사를 효율적으로 지원" 이며, 이를 위해 약 수 년간 각종 소프트웨어 및 알려진 파일을 수집하고 이에 대한 정보와 해시 검색 기술의 인프라를 구축하자, 미국 내의 컴퓨터 포렌식 관련 산업계가 이를 적극 활용하고 현장에 적용하고 있다.

2.4 증거제출

□ 무결성

디지털 증거 무결성 확보기술은 증거 자료의 신뢰성을 확보하기 위해서, 수집된 데이터가 변조 및 손상되지 않았음을 해시 및 오류 검증 알고리즘을 이용하여 증명하는 기술이다. 이는 입수된 디지털 증거가 법적으로 제정된 디지털 포렌식 표준 절차 및 기술이 필요하다.

□ 포렌식 툴 검증

디지털 포렌식에 사용되는 포렌식 툴에 대한 인증이 없이는 포렌식 툴에 의해서 얻어진 분석 결과를 믿을 수 없는 것은 자명하다. 디지털 포렌식 툴의 검증을 위해서 미국에서는 미국 국립표준기술연구소(NIST)에서 디지털 포렌식 툴 검증(CFTT)을 시행하고 있다[7]. CFTT에서는 디지털 포렌식 툴의 검증 및 평가 방안을 제시하고, 평가 결과 보고서는 미국의 국가 법무연구소(NIS)와 함께 공동으로 발간하여 일반인들도 쉽게 열람할 수 있도록 하고 있다. 컴퓨터 범죄 수사관들은 이 보고서를 참조하여 디지털 포렌식 툴의 선정 기준을 확립하며, 변호사와 검사들은 디지털 증거의 객관성을 증명하기 위한 자료로 활용하고 있다.

2.5 포렌식 시스템 및 툴 현황

현재 상용화되어 잇는 컴퓨터 포렌식 증거 수집 및 분석 소프트웨어는 Guidance Software사의 EnCase와 AccessData사의 ForensicToolkit이 가장 널리 사용되고 있다. Paraben사는 모바일 기기에 대한 전문 분석가들을 위해서 Cell Siezure, PDA Siezure 등의 소프트웨어와 각종 휴대용 기기와의 연결을 지원하는 툴박스 형태의 상용 제품을 제공하고 있으며, 메모리를 직접 분석 할 수 있는 소프트웨어도 개발하여 제공한다. 포렌식 툴의 현황은 <표1>과 같다.

〈표 1〉 컴퓨터 포렌식 기술 연구 현황

도구 이름	지원 운영체제	공개 여부	이미지 생성 및 검사	무결성 검사	저수준 복구	기타 지원 기능
ForensicX	Unix/Linux	Com	Disk, OS, Traffic	Hard, File, Finger	Delete	Plug, Report
MaresWare	Windows	Com	Disk	Hard, File		
	Linux	Com	Disk	File		
The Coroner's Toolkit	Unix/Linux	Free	Disk	Hard	Delete, Key	
Tom's Rootboot	Linux	Free	Disk, OS			Boot
EnCase	Windows	Com	Disk, OS	Hard, File, Finger	Raw, Delete	Plug, Report
Byte Back III	Windows	Com	Disk, OS, Traffic	Hard, File	Raw, Delete	
ForensicToolkit	Windows	Com	Disk	Hard, File	Raw, Delete	Report

주 1) 공개여부: Com(상용), Free(공개용)
2) 이미지 생성 및 검사: Disk(디스크 이미지), OS(운영체제 이미지), Traffic(IP 트래픽 이미지)
3) 무결성 검사: Hard(하드웨어 변동 검사), File(파일 무결성 검사), Finger(전자 지문 검사)
4) 저수준 복구: Raw(저수준 파일 편집), Delete(삭제 파일 복구), Key(암호키 복구)
5) 기타 지원 기능: Boot(긴급 부팅 지원), Plug(플러그인 지원), Report(자동보고 지원)

2.6 포렌식 활용 분야

□ 수사기관

검찰, 경찰, 국정원, 기무사 등에서는 스파이, 기술 유출, 공갈, 사기, 위조, 해킹, 사이버 테러와 같은 컴퓨터 범죄수사 분야에 활용하고 있다.

□ 기업체

회사 정보 및 기술 유출은 모든 종류의 기업체에서 발생하고 있으며, 이로 인하여 측량하기 어려운 손해가 발생하고 있다. 따라서 증권, 보험, 은행 등의 금융회사를 포함한 일반회사에서도 금융사고, 회계감사 및 정보유출 등의 보안사고 발생시 민·형사상 책임소재를 가리기 위한 증거자료 확보를 위해 컴퓨터 및 모바일 포렌식 기술을 활용할 수 있다.
미국에서는 2007년 말부터 증거공개명령제도를 시행할 예정이며, 미국에서 경영활동을 하는 글로벌 기업들은 국내법처럼 준수해야 한다.

□ e-discovery

미국에서는 디지털 증거에 대한 제출을 정다화하는 e-discovery 제도가 시행되어 2006년 12월에 통과되었다.
따라서 민·형사 분쟁 발생시 방대한 양의 디지털 자료로부터 분쟁에 필요한 자료를 효율적으로 추출하는 포렌식 툴이 필요하다.

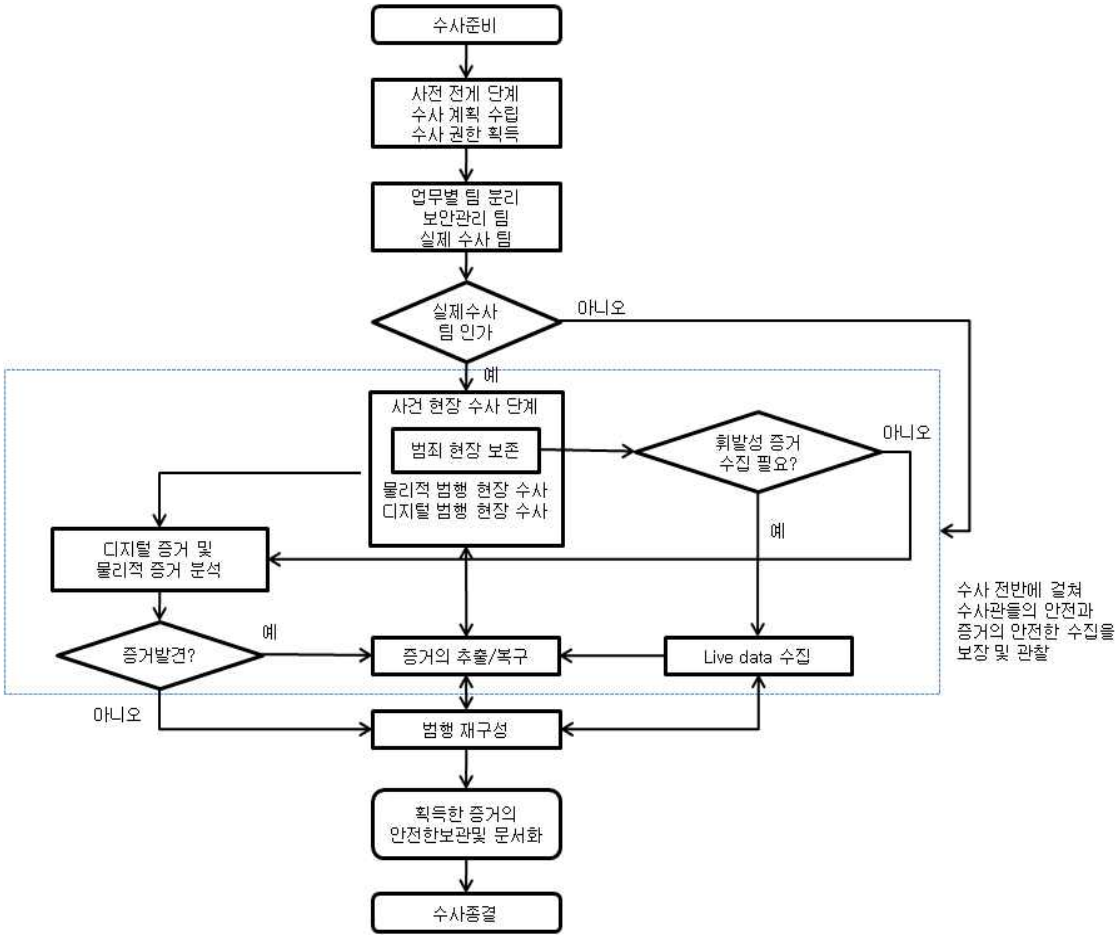
2.7 포렌식 발전 방향

디지털 포렌식이 유용하게 사용되기 위해서 해결 되어야 하는 문제점들은 다음과 같다.
첫째, 포렌식에 의해 얻어진 디지털 증거를 법적 증거로 채택하기 위해서는 형사소송법상의 증거문제 해결이 필요하며, 포렌식 절차에 관한 표준화가 필요하다.

또한 여러 포렌식 툴간의 호환성을 위해서는 포렌식 이미지의 포맷에 대한 표준화가 필요하다.
둘째, 포렌식 대상이 되는 디지털 데이터는 점점 대용량화되어 가고 있으므로 포렌식 이미징을 만드는 작업이나 검색작업 등이 고속화되어야 하며 이에 대한 연구가 필요하다.
셋째, 외산 포렌식 장비를 사용할 경우 국산 디지털 파일들을 분석하는 기능이 부족할 수 있으며, 국내 사법 제도 등 국내 환경에 대한 특성이 반영되지 않아 수사상 어려움이 존재할 수 있으므로 국내 실정에 맞는 포렌식 장비의 개발이 필요하다.
넷째, PDA, 핸드폰, 디지털 커메라, 캠코더 등 다양한 형태의 디바이스가 새로 나오고 사용되고 있으므로 다양한 형태의 디바이스에 대한 포렌식 툴 개발이 함께 진행되어야 한다.
위에서 언급한 여러 문제점들이 해결되면 디지털 포렌식은 현재 활용되고 있는 분야 이외에도, 디지털 증거의 인증 서비스와 같은 새로운 보안 서비스 시장을 창출하거나 활성화 시킬 수 있으리라 예측된다.

3. Encase를 이용한 Digital Forensics

3.1 Interactively Unified Invesigation Model



□ 수사 준비 단계

- 이 단계는 수사를 본격적으로 진행하기 전에 현재 의 기술 및 동향에 맞는 디지털 포렌식 수사 도구를 구비하고, 수사에 투입될 인력에 대해 사전 교육을 행하는 단계이다. 그리고 특정 범죄가 발생한 시점이 아니더라도 CCTV 같은 보안 인프라를 구축해 놓는 단계이기도 하다. 이러한 디지털 포렌식 수사의 준비 과정은 유/무형의 수사 자원을 wnsqlgkadmfhTJ 수사 내 외부적으로 여러 이득을 얻을 수있다.

□ 사건 전개 단계

- 사건이 발생했을 때 그에 대한 신고와 탐지를 바탕으로 현장에 대해 최대한의 정보를 수집함으로서 해당 사건을 범죄 화 시킬 지에 대해 결정하는 단계이다. 최대한으로 정보를 수집해야 하므로, 간계의 특성상 사건 현장을 수사하는 단계와 상호작용이 필수적이다. 이 단계의 결과를 바탕으로 압수 혹은 수색 영장을 발부 받을수 있다.

□ 업무별 팀 분리 단계

- 수사관들이 범랭 현장에 도착했을 때, 최우선으로 고려해야 할 것은 '안전'이다. 이는 수사를 진행하는 수사관들의 안전 뿐 아니라 수색 및 수집 대상인 증거의 안전도 동시에 뜻한다. 안전을 보장하기 위해서는 수사관들이 각자가 맡은 증거 획득에 집중하는 것과 동시에 수사관들이 통제된 주변 상황 속에서 안전하게 증거를 수집할수 있고 수사관들이 수집한 증거가 안전하게 획득하고 보관되고 있는 지를 관리하는 팀이 필요하다. 위와 같은 업무를 수행하는 '보안 관리팀'과 실제 현장 수사를 진행하는 '실제 수사팀'으로 팀을 구성한다. 실제 수사팀은 '사건 전개 단계'에서 수립된 수사 계획에 EK라 치밀하게 수사를 진행하고 보안 관리팀은 실제 수사팀의 수사 상황을 관리 하고 수사관과 증거의 안전을 보증하도록 한다.

□ 사건 현장 수사 단계

- 사건 현장을 대했을 때 가장 중요한 것은 그 현장 을 보존하는 것이다. 현장을 보존한다는 것은 차후 원활한 수사 진행을 위해 범행 현장 및 잠재적인 증거를 확보하는 의미이므로 매우 중요한 단계이다. 현장의 상황에 대한 간단한 노트, 사진 촬영, 태그 붙이기 및 스케치를 할 수 있는데 현장에 있는 수집 대상물의 위치를 상세히 기록하여야 한다. 확보된 범죄 현장을 확인하고 증거를 수집한 뒤 범행 현장의 범위를 한정할 수 있기 때문이다. 디지털 증거를 획득하기 위해서는 우선 어떤 종류의 증거를 획득할 것인가에 대해 명확히 해야 한다. 네트워크, 응용 프로그램, 파일 시스템, 웹 등 과 같이 목적에 따라 분야별로 전문화된 접근을 통한 적합한 수사를 수행하여야 한다. 또한 범죄 현장에서 수집된 증거 는 해쉬, 값을 이용하거나 혹은 분석용 이미지를 생성하여야 한다.

□ 휘발성 증거 수집 단계

- 시스템의 메모리에 임시로 저장 된 데이터를, 유사하게 휘발성 증거라 하며 현재 시스템이 작동 중인 상태에서의 데이터를 의미한다. 이는 라이브 시스템 상태에서 획득이 가능한 정보들이 많이 존재하므로 간과해서는 안된다.

□ 증거의 추출/복구 단계

- 획득한 여러 증거로부터 법정에 명확한 근거를 가진 증거를 추출해 내고 그로부터 범죄 현장을 복구하는 단계이다. 증거를 추출함에 있어서는 그 대상에 따라 그 방법이 달라질 것이다. 즉, 네트워크, 응용 프로그램, 파일 시스템, 물리적 매체 혹은 각종 문서 중 어떤 것에서 증거를 획득 할 것이냐에 따라 증거 추출 방법은 달라질 수 밖에 없다. 이 과정에서는 민감한 정보에 대해 합법적으로 접근하기 위해 법적으로 충분한 접근 권한을 획득한 후 심층적으로 증거 수집을 진행해야 한다.

□ 범행 재구성 단계

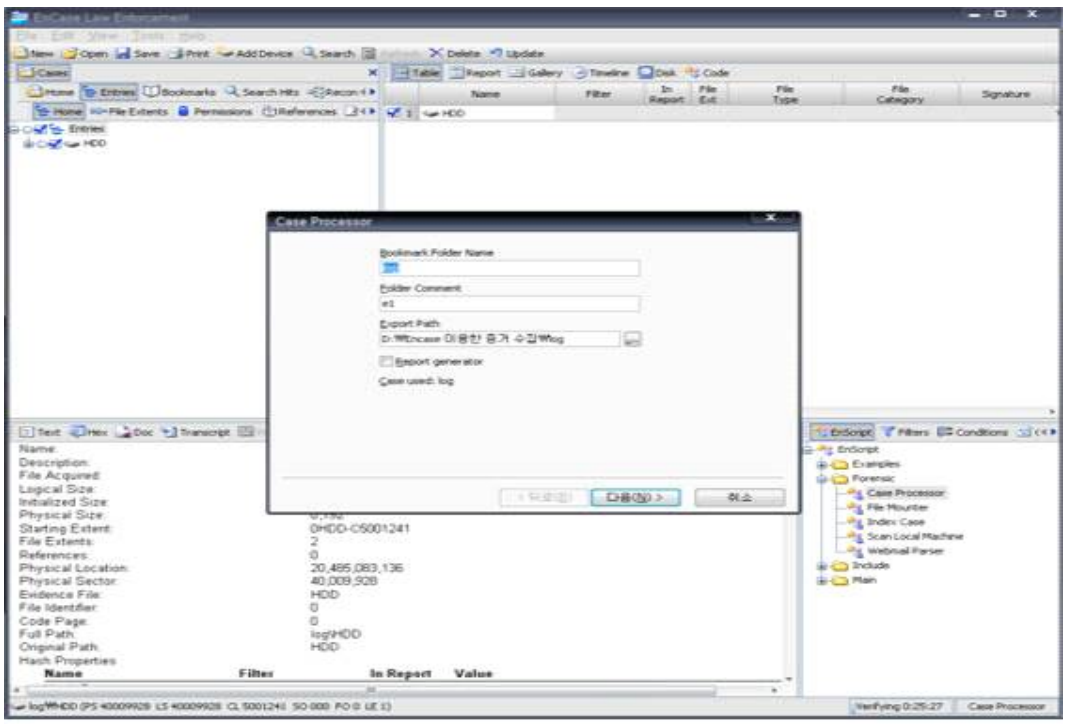
- 이전 단계들로부터 수립된 증거들을 이용하여 범행의 실체를 재구성하는 것이 매우 중요하다. 범행을 재구성하는 그 자체뿐만 아니라 추후에 그 범죄가 어떻게 행해졌느냐에 대한 프로파일링 역시 중요하다.

□ 획득한 증거의 안전한 보관 및 문서화 단계

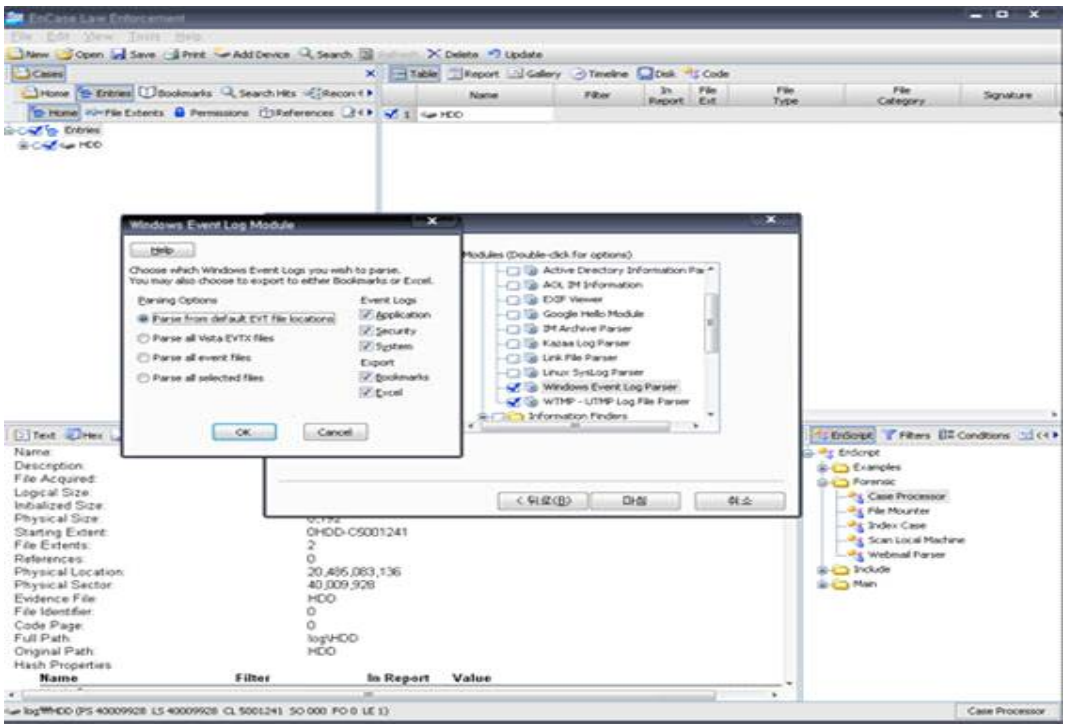
- 증거를 발견하고 결정적인 증거를 추출해내는 것 못지않게 증거를 안전하게 보관하고 증거를 법정에서 효력을 발생할 문서화 하는 것 또 한 중요하다. 양질의 증거를 획득 했으나 원본 증거를 훼손 하여 법정에서 증거의 무결성이 지켜지지 않았다하여 소송이 기각된 사례는 많다. 획득한 증거에 해쉬 등의 무결성을 입증할 수 있는 값을 부여하고, 적절한 방법으로 안전 한 곳에 보관해야 한다.

3.2 Log 분석 시나리오

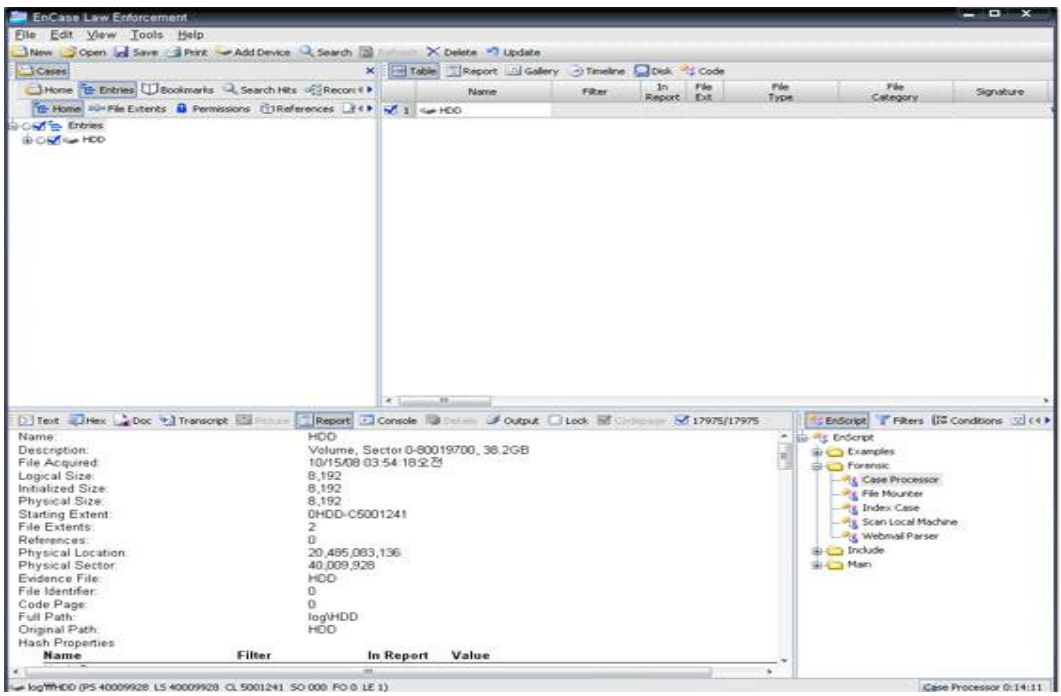
□ 포렌식의 툴 을 이용하여 windows 이벤트 로그 분석 가능, 디지털 증거 수집 절차에 따라서 원본 HDD를 이미징 한다. 이미징 완료된 HDD를 가지고 아래 그림 처럼 포렌식 툴에 마운트 하여 이미지를 불러 드린다.



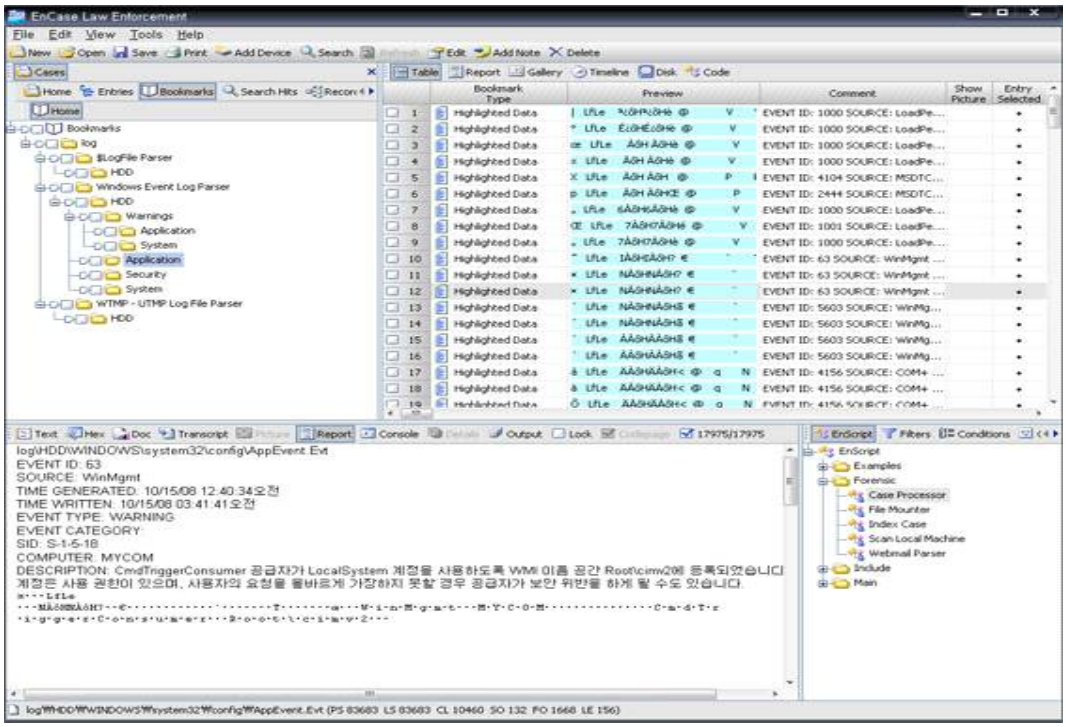
□ 포렌식의 EnScript 기능을 이용하여 원하는 log를 선택하여 아래와 같은 그림처럼 설정을 한다. 단 주위 할 점은 Log 분석은 위에서 설명 한것처럼 증거 수집 방법중 라이브 시스템이 아닌 데드 시스템이라는 점을 명시한다.



□ EnScrip의 Case Processor을 이용하여 위 명령을 실행 하면 아래 와 같은 형식의 조사 과정을 확인 할 수 있다. 현재 화면 상에서는 Log 분석에 필요한 시간은 14분 정도로 표기 된 것이 보일 것이다.



□ 경과 된 시간을 확인 하면 아래와 같은 그림 처럼 포렌식의 View 기능을 통하여 Windows 이벤트 로그인을 확인 할 수 있다. 아래 그림 처럼 접근자 Evevnt ID, 작동 시간 그리고 SID, 이벤트 내용을 확인 할 수 있다.



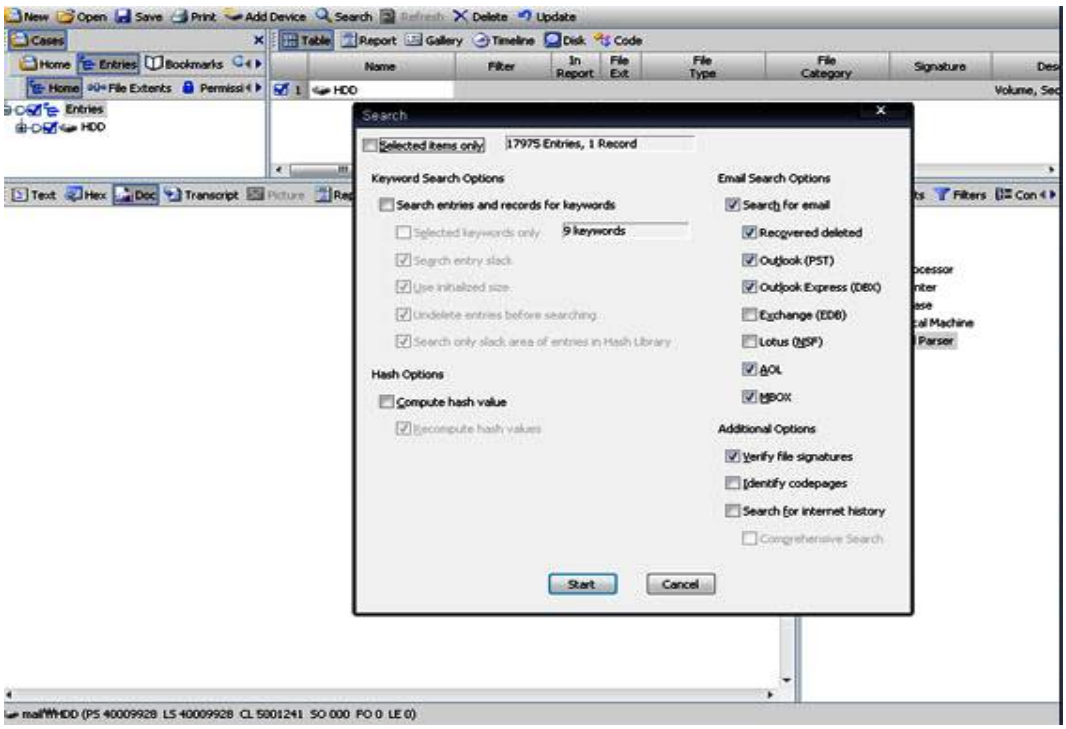
□ 범죄 수사시 윈도우 로그는 본 논문에서 설명 한 것 처럼 라이브 시스템 과 데드 시스템 상에서 가능 하다는 점을 알 수 있다. 각 각의 Log 분석시 차이점은 크게 없으나, Log의 정확한 정보를 확인 하기 위해서는 라이브 시스템을 사용 하는 것이 유용하다. 라이브 시스템은 데드 시스템과 달리 현재 작동 상태의 log를 확인 가능하다고 다른 참고 자료나 논문에서 알 수 가 있다.

또한 log 은 범죄 수사 시 중요한 역할을 하나 단점으로는 이벤트 log에 대한 사용자의 임의의 삭제 시 일반 적인 포렌식 절차로는 복구하기가 힘들다는 단점을 가진다. 그렇기 때문에 log는 라이브 시스템 상태에서 확인을 요망하는 작업이기도 하다. 운영체제 자체 적으로 log를 확인 가능하나 증거 제출시 포렌식을 이용한 자료가 아닐 경우에는 법적 효력이 없다는 점을 가만할 경우, 라이브 시스템이나 데드 시스템 분석시 필히 검증된 포렌식 툴을 이용해야 한다.

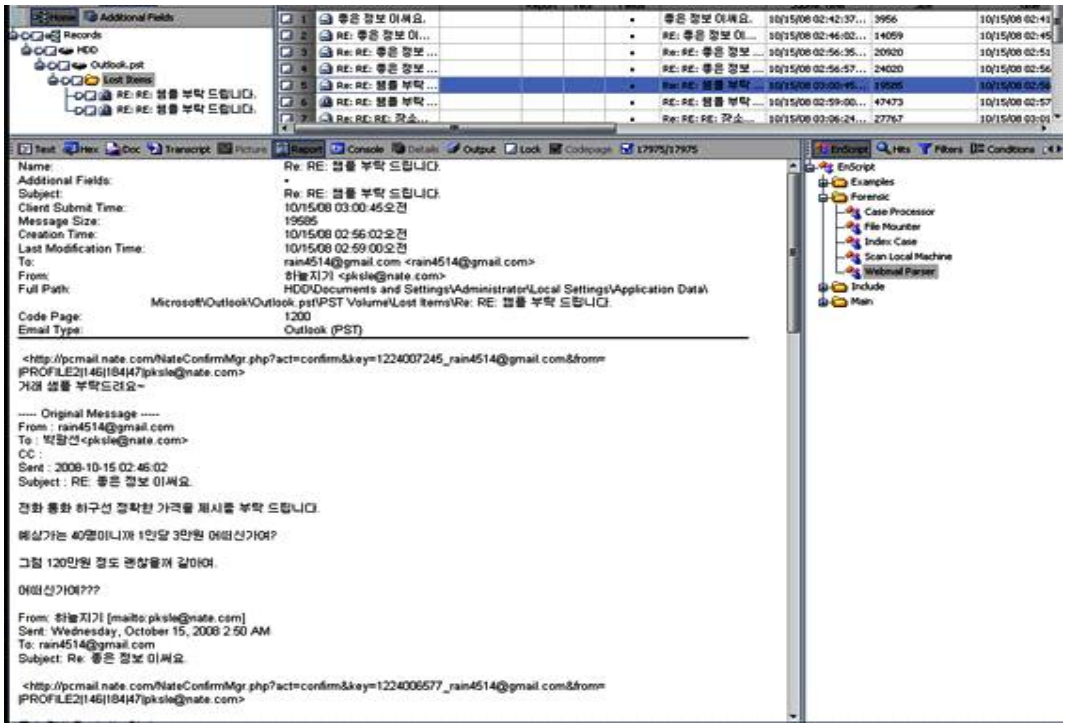
3.3 E-mail분석

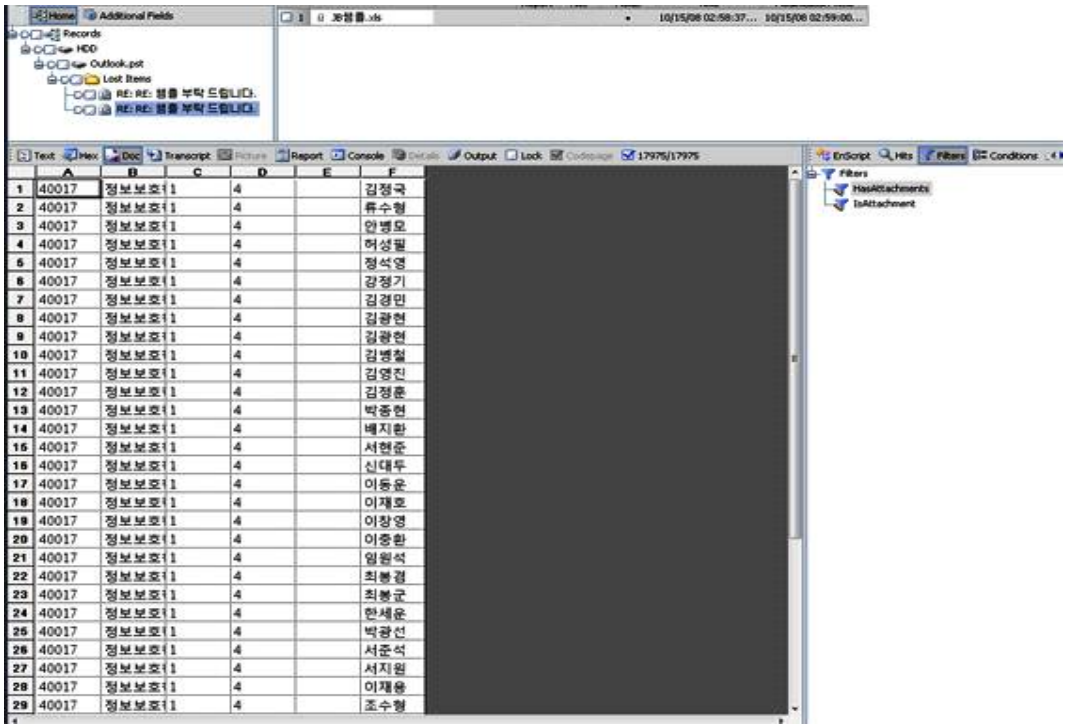
□ 포렌식 툴 중 가장 사이버 행위를 파악하기 위한 툴 중 하나로 E-mail 분석이다. 이 기법은 얼마 전 이슈화 되었던 “신”씨의 사례를 예를 들 수 있다. “신”씨는 국내 고위 관계자들에게 로비를 하며, E-mail일 전송을 주로 한 것으로 들어 알려져 있다. 하지만 그때당시 포렌식의 중요성을 정보통신 사회에서는 인식을 하지 못하였으나. 이 사건의 계기로 우리 나라 정부기관도 포렌식에 대한 중요성을 인식한 것으로 알고 있다.

□ 아래 그림처럼 포렌식을 이용해서 Outlook 등의 이메일분석이 가능 하다.
이번 사건은 시나리오 형식으로 설명을 하자면, 최근 이슈화 되어 문제가 된 개인정보 유출을 예로 들어 볼 수가 있다.
사이버 수사대는 용의자로 의심되는 인원의 PC의 기억매체인 HDD를 압수하여 이미징 한뒤 아래의 포렌식 툴 중하나인 Seach를 기능을 이용하여 삭제된 Outlook의 PST, MBOX를 복구 가능 하다.



□ 분석이 완료되면 아래 그림처럼 포렌식 툴의 Record 탭에서 아래와 같은 형식의 분석 결과를 확인 가능하다. 정보 유출자와 거래 인 간에 E-mail을 주고 받으면서, 언제 어떻게 어느 회사의 E-mail을 이용하여 거래를 한 것을 확인이 가능하다. 하지만 이러한 상황으로는 증거가 부족하기에, 다음 그림인 개인 정보에 관한 자료가 첨부된 E-mail 을 주고 받은 것을 확인으로 정확한 증거 수집 가능하다.



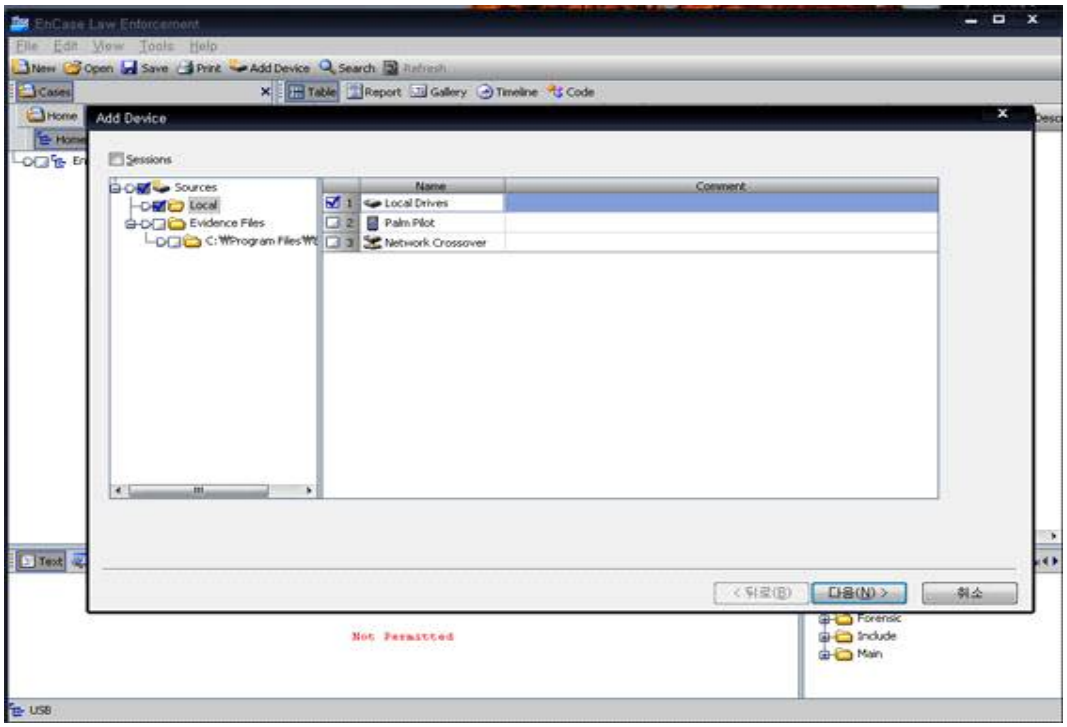


3.4 USB 분석 시나리오

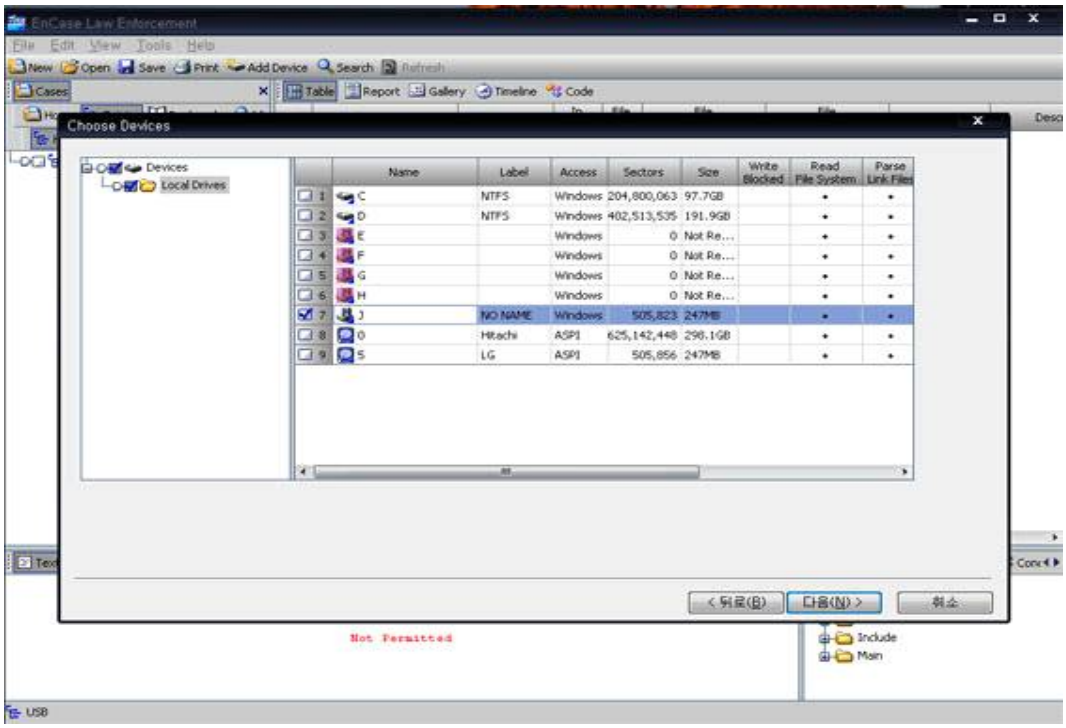
□ 다음으로는 일반 적으로 가장 현대 사회속에서 많이 사용되는 USB를 이용한 범죄 분석이다. USB 정보화 사회가 되면서 기존에 디스켓이나 CD를 이용한 파일 및 자료를 저장 또는 가지고 다니던 시대를, 현대 과학의 기술 발전으로 휴대가 용이하며 컴퓨터만 사용가능한 장소이면 시간과 장소에 구애 받지 않는 장비중 하나이다. 하지만 이러한 점을 이용한 사이버 범죄는 증가율은 높아간다. USB를 이용하여 중요한 기업의 정보 또는 개인 정보를 유출이 가능해 지기 때문이다. 기업내에서는 내부망을 사용하기에 자신이 유출할 정보를 전송하기가 까다롭다. 하지만 USB는 내부망 이라고 할 지언즉 USB 단자만 사용 가능 하다면 언제 어디서나 사용이 가능하다.

아래 그림은 범죄 수사시 사이버 수사대에서 무결성을 입증하기 위해 USB의 이미징 하는 순서와 범죄 수사 과정을 나타 낸다.

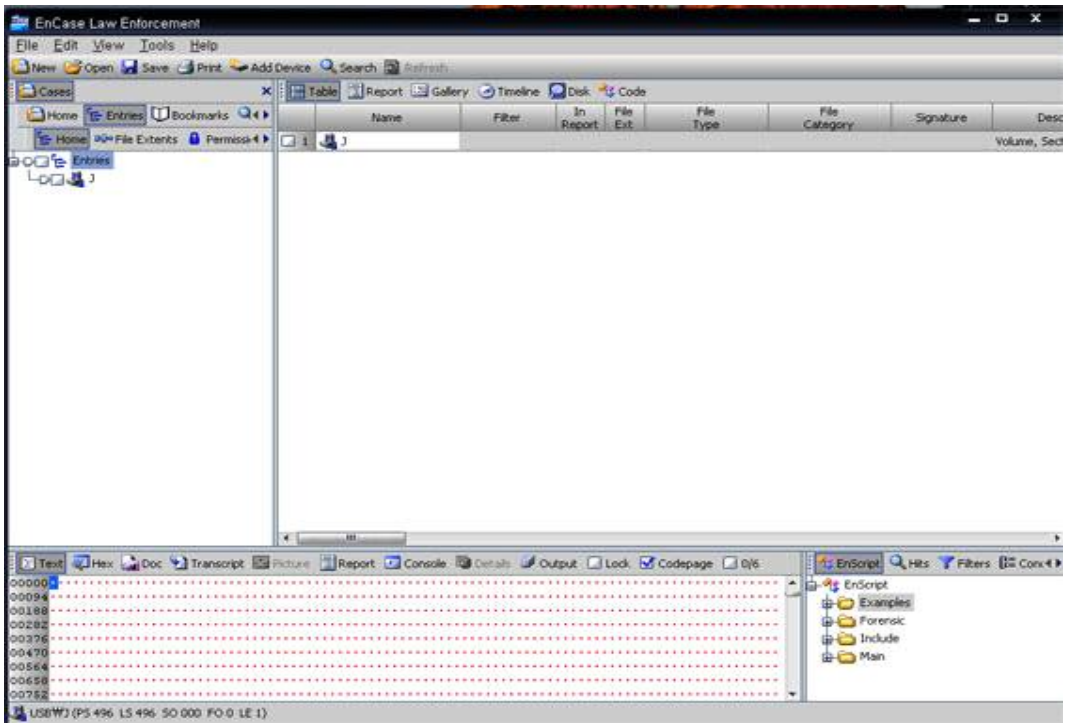
1) USB의 무결성 입증을 위한 이미징



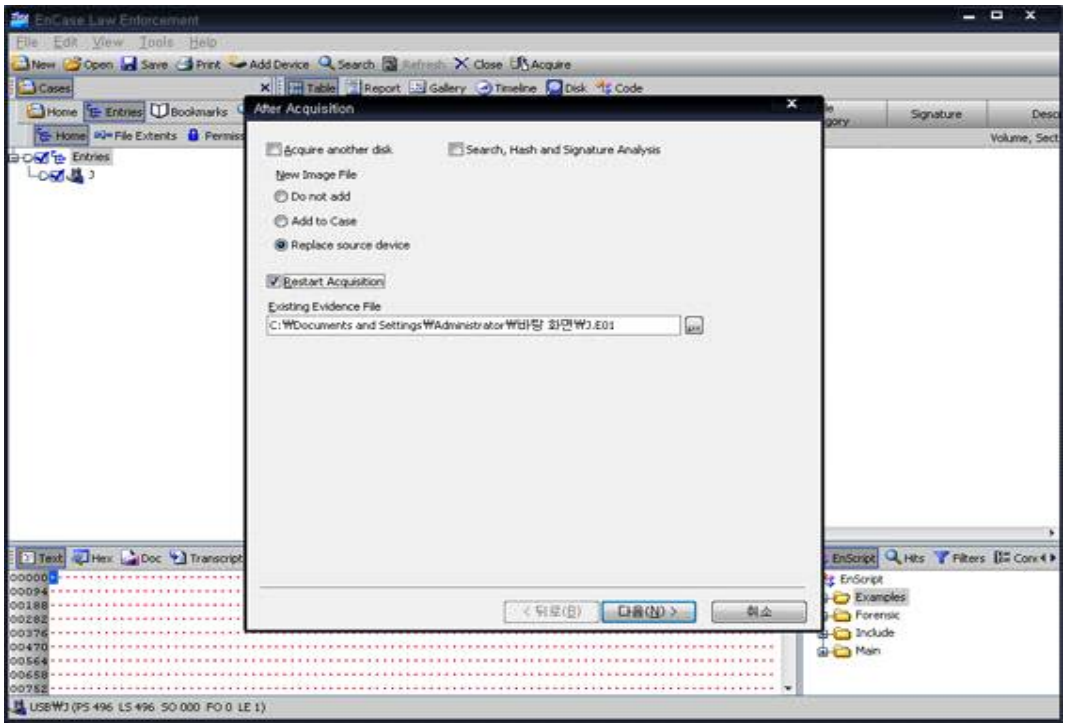
2) 이미징 하기위한 저장 매체 선택



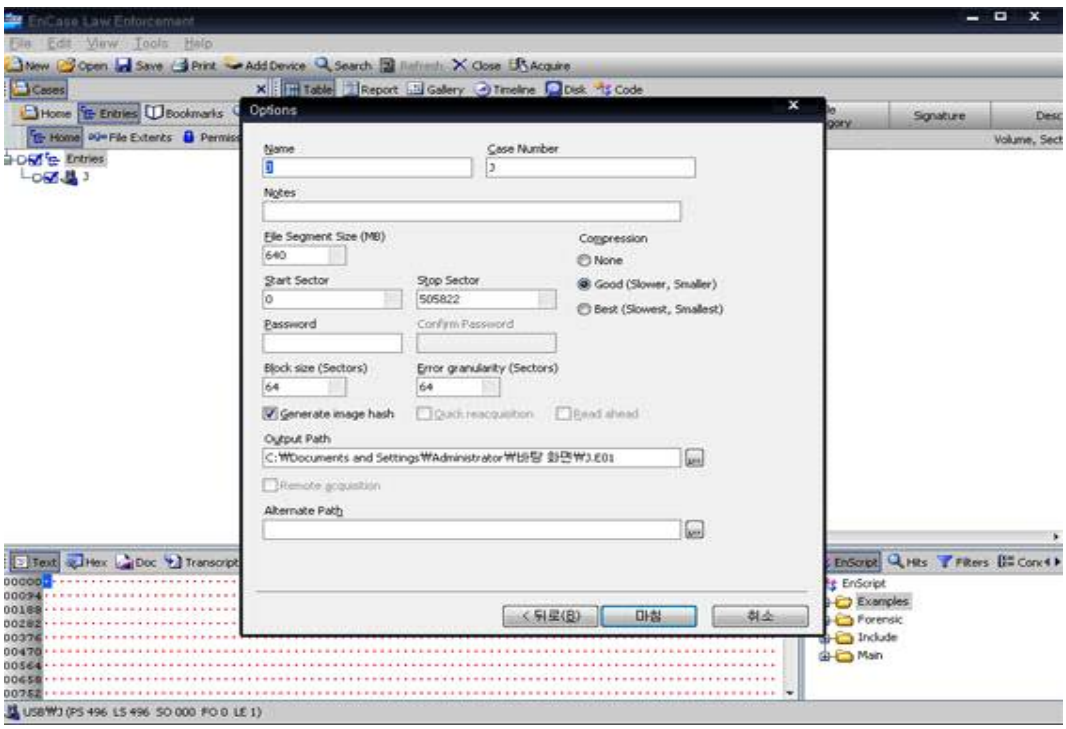
3) 저장 매체를 선택 하면 아래 의 그림 처럼 Entries 메뉴 Home에 마인틴 확인



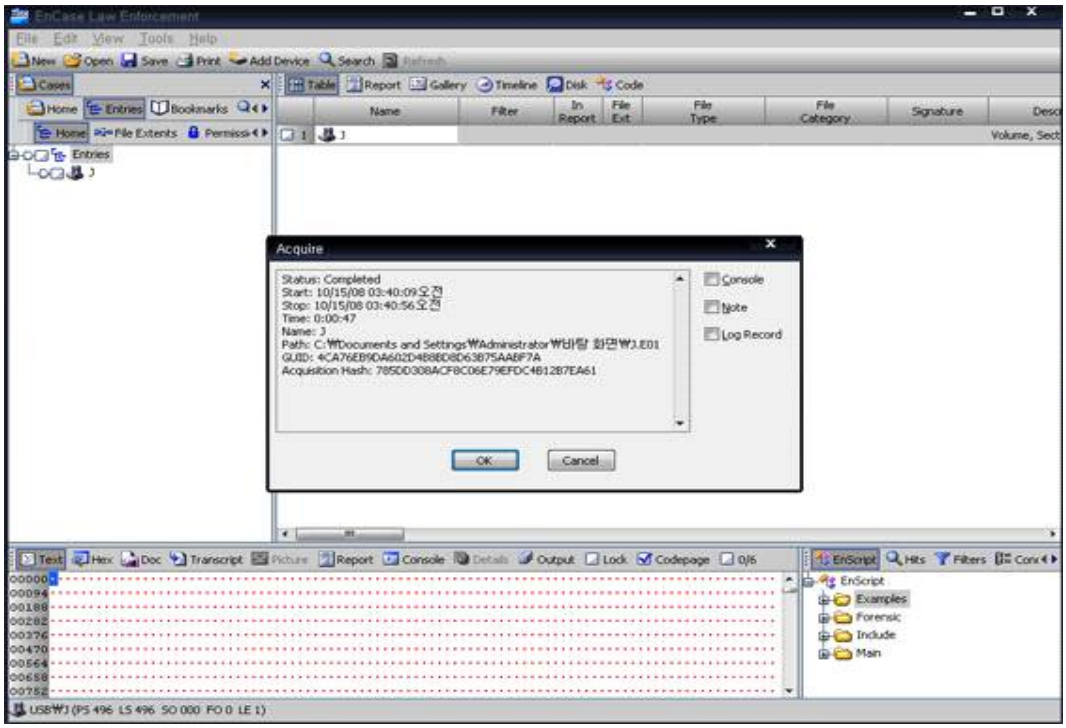
4) 마운틴 된 저장 매체를 선택하고 Acquire를 선택 하여 아래 그림 처럼 저장 위치와 옵션을 선택한다.



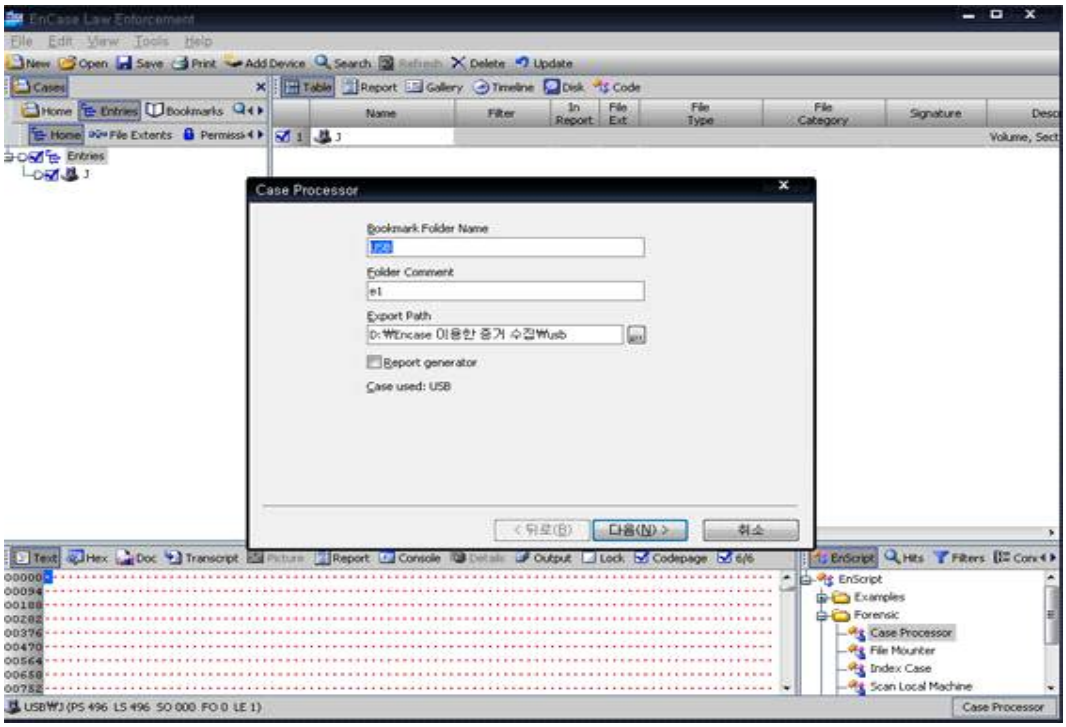
5) 옵션을 선택하면 본 화면 처럼 이미징 name과 무결성을 입증 하기 위해여 저장 매체의 password 및 저장 위치를 선택 가능 하다.



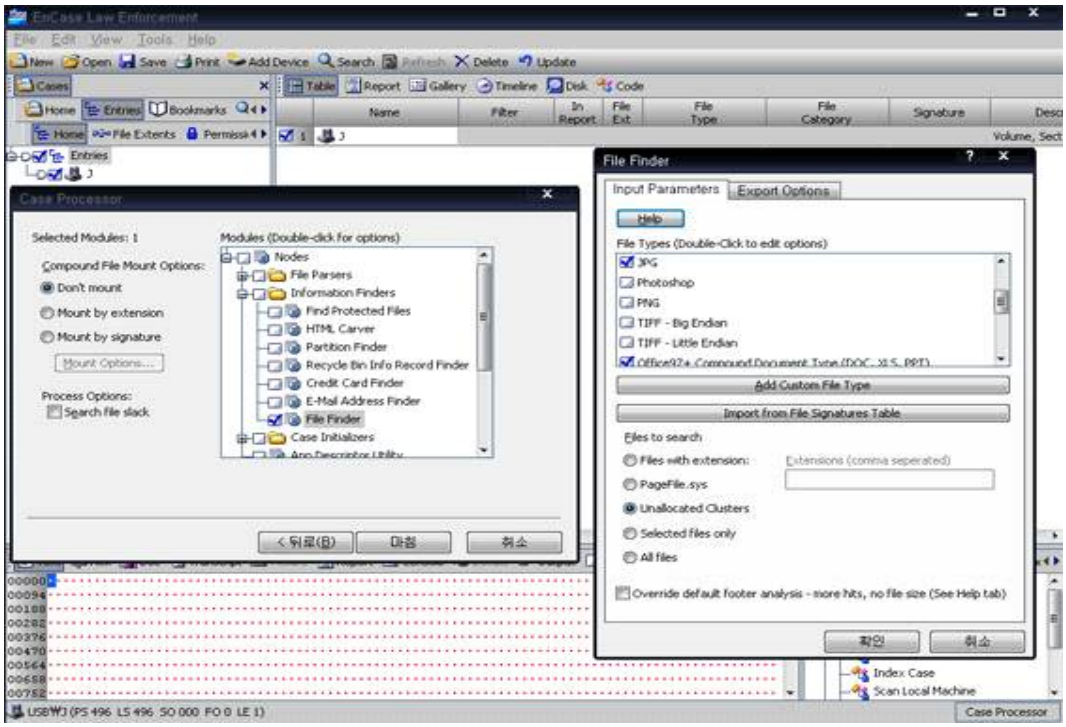
6) 이미징이 완료되면 Acquire의 작업 완료 내용과 이미징 생성 날짜 확인.



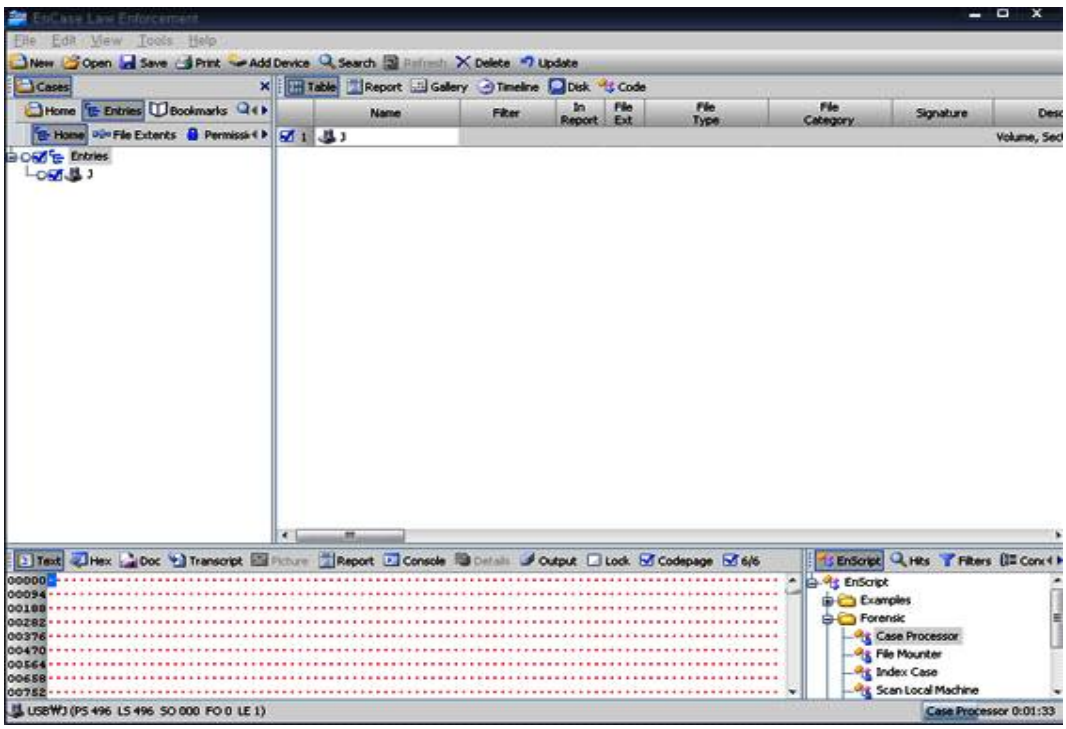
7) 아래의 그림은 포맷된 USB의 복구를 위한 설명을 나타 낸다.
EnScript의 Case Processor를 선택 하여 저장 위치와 폴더 명을 선택



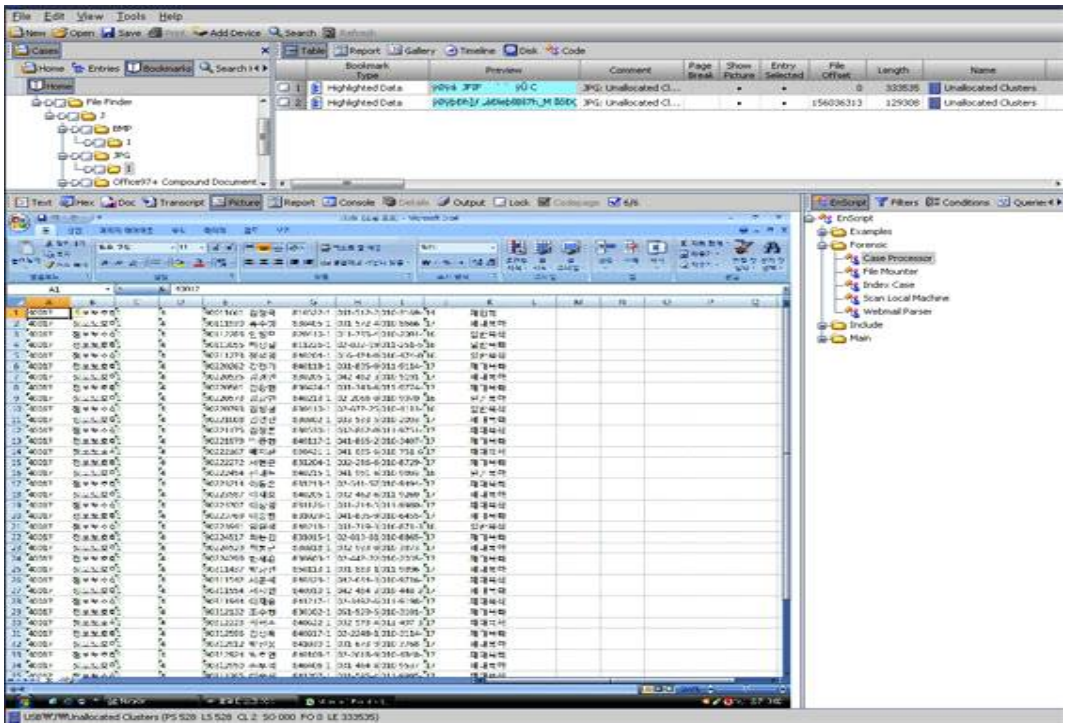
8) Case Processor의 옵션중 파일 삭제를 한 경우 증거 수집 확률이 높은 Filefinder를 선택 하고 증거 수집을 하고자 하는 확장자를 찾아 선택 한다.



9) 선택이 완료되면 Case Processor의 진행 상황 과 남은 시간을 확인 가능



10) Case Processor 의 증거 수집 절차가 완료되면 포맷을 통해 삭제된 파일의 증거 수집 완료 하여 삭제된 파일의 원본을 확인 하여 원본과 비교 한다.



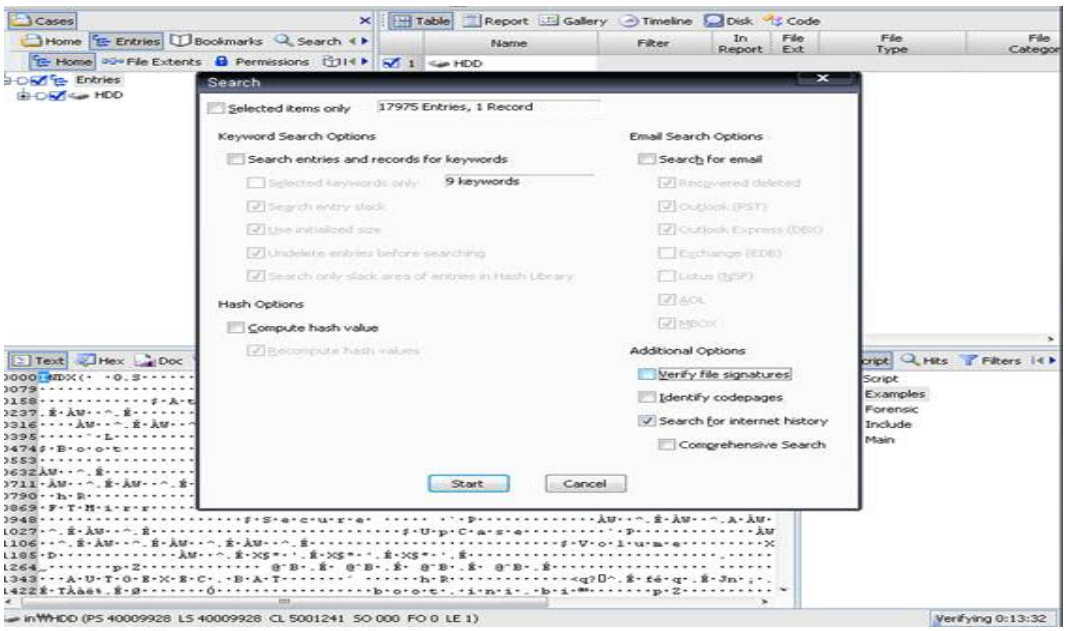
11) Case Processor의 Filefinder의 기능이 삭제된 파일에 대한 증거 수집에서 많이 사용 된다고 하지만 몇 가지의 단점을 가진다. 첫째 대용량의 저장 매치 분석이에 대한 소요 시간이 길다는 단점을 가진다. 둘째 디지털 포렌식 검증 툴에 따라 삭제된 파일의 복구율이 랜던 하다는 단점을 가진다. 예를 들면 Encase는 hwp를 지원 하지 못하며, hwp와 일종의 기본적으로 지원하지 않는 확장자는, 커스텀 옵션을 통하여 확장자와, 헤더값을 알아야 증거 수지이 가능하다. 마지막으로는 Filefinder를 사용 하더라도, 본문에서 설명한 것 처럼, 저장 장치를 fdisk 또는 포맷 후 클러스트에 다른 파일이 저장 된다면 복구 율은 현저희 줄어들며, 이번 연구에서 사용한 Encase는 아쉽게도, 확장자가 xls, ppt인 파일은 복구 율이 저조 하다는 점의 단점을 가진다.

정부 기관에서는 증거 수집 절차에서 검증 된 포렌식 툴을 사용하며, 한가지의 툴 만을 이용해서 검색을 하는 것이 아니기에 검색 율 과 증거 수집에 용이 하지만, 포렌식 관련 툴이 고액이라는 단점으로 인하여 디지털 포렌식 관련 연구를 하는 연구원들에게는 가장 큰 단점을 가진다.

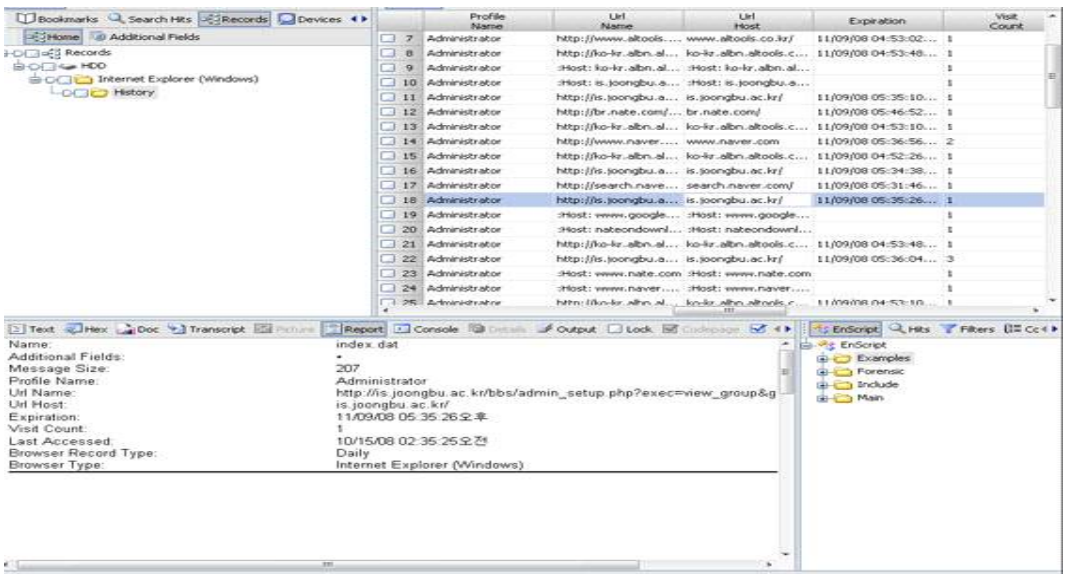
3.5 인터넷 History

□ 디지터 포렌식의 툴 중 하나인 인터넷 History 기능은 증거 수집 시 큰 역할을 한다. 최근 이슈화 된 개인 정보 유출 관련을 사례로 들어 보면, 브로커와 접촉하기 위하여, e-mail을 보내기 위하여 포털 사이트를 접속하거나, 또는 관련 자료를 검색하기 위하여, 어떤 경로를 통한지 정보를 수집 가능 하기 때문이다. 또한 Search 기능을 통하여 삭제된 History를 복구 가 가능하다.

1) Search를 이용하여 Search fot internet history 옵션을 체크하여 간단하게 인터넷 History 검색이 가능하다.



2) 검색된 History를 통하여 is.joongbu.ac.kr 접속한 것을 확인이 가능하다. 접속한 시간과 날짜, 어떤 인터넷 접속 프로그램을 사용한지 확인 가능 하다.



4. 결 론

우리나라는 정보 인프라의 구축을 위해 과감한 투자를 해왔고 이제는 그러한 발전에 힘입어 전 세계 IT 분야를 선도하며 도약하고 있다. 이러한 정보기술의 발전과 하드웨어의 첨단화에 따라 법정에서 가장 중요한 증거도 대부분 디지털화 되고 있다. 미국 FBI에서“현대 사회의 기업에서 생산되는 정보의93%가 디지털 형태로 생산된다.”고 발표한 바 있다. 수사기관이 수집하고 법정에서 활용되는 거의 모든 증거가 디지털 증거라고 할 수 있을 정도이며, 또한 수많은 컴퓨터와 네트워크가 디지털 증거를 저장하는데 사용되고 있다. 따라서 이를 입증하는 방법으로 법정 제출용 디지털 증거를 수집하는 기술인 디지털 포렌식이 필요하게 되었다.

□ 디지털 포렌식 산업 육성 방안

디지털 포렌식 기술이 활용되는 산업 분야는 크게 포렌식 소프트웨어 산업과 하드웨어 산업으로 분류 될 수 있다. 포렌식 하드웨어 산업 분야는 법정 제출용 디지털 증거의 훼손을 방지하는 장치를 개발하는 분야이다. 예를 들면, 전자매체에 기록된 데이터를파괴할 수 있는 자기장으로부터 분리가 가능한 장치, 하드디스크를 빠른 속도로 복제할 수 있는 장치, 디지털 증거의 훼손 없이 오랜 기간 저장할 수 있는 장치, 개인 분석용 포렌식 관련 기능이 내장된 서버, 이동성을 가지고 현장으로 휴대하고 가서 분석가능 하고 다양한 기능을 제공하는 포렌식 가방 등 새로운형태의 장치 개발이 절실히 요구된다. 포렌식 소프트웨어 산업 분야는 법정 제출용 디지털 증거의 수집 및 분석을 위한 여러 가지 소프트웨어를 개발하는 분야이다. 주로 현장에서 증거의 수집, 증거의 분석, 증거의 무결성 입증, 증거의 분석과정의 연속성 기록, 디지털 포렌식 전과 정에 대한 보고서 작성 등을 위한 소프트웨어의 개발이 요구된다. 현장에서 확보된 데이터로부터 정제를 통해 유용한 증거를 추출하기 위하여 저장매체에서 삭제된 파일 복구, 키워드 혹은 자연어 기반의 검색, 다양한 단어를 분류하고 정렬하는 인덱싱, 원본의 수정 또는 변경 없는 복제, 로그 기록 및 분석 기술 등이 디지털 포렌식에서 요구되는 주요 소프트웨어 기술이라 할 수 있다.

이와 같이 저장매체, 운영체제, 데이터베이스, 네트워크 기술 등 기존의 IT 기술이 포렌식과 연관성을 갖고 디지털 포렌식 영역내에서 포렌식 기관의 수요에 맞는 형태로 적응하여 발전되어야 한다. 국내의 디지털 포렌식 산업은아직 시작단계에 있으며 아직 해결해야 할 과제가 많다. 첫번째, 법정에서 객관성이 인정되고 또한 주로 사용되고 있는 디지털 포렌식 도구들은 대부분 미국 등 국외에서 개발된것들이다. 국내에서도 관련 기술 개발이 시작되었으나 실제 디지털 포렌식 산업 분야에서 활용될 수 있는 신뢰성 높은 도구의 개발을 위해서는 정부 차원의국산화 지원 정책이 요구된다. 두번째, 검찰청, 경찰청 등의 수사기관의 폐쇄적 성향으로 인해 기관 간의 협조 체제가 미비하다. 각 기관마다 디지털 포렌식 기술 개발을 위한 독자적인정책을 수립하여 추진 중이나 법원, 검찰청, 경찰청,국정원, 감사원 등의 관련 기관들이 중복 투자를 줄이고 디지털 포렌식 산업의 활성화를 앞당기기 위해서는 서로간의 대화와 협의를 통해 국가적 차원의 관련 표준 개발 및 법제도 강화에 힘을 모아야 한다. 포렌식 증거력에 대한 최종 판단을

하는 법원의 의견 뿐만 아니라 소추 제기를 전담하는 검찰청, 수사를 담당하는 검찰, 경찰, 국정원, 기무사 등 각 기관의 의견이 모두 반영된 표준화 모델이 만들어져야 할 것이다. 세번째, 기술적으로 복잡하고 난해하여 디지털 포렌식을 위한 분석가의 전문성이 매우 중요함에도 불구하고 국내 디지털 포렌식 전문 인력은 상당히 부족한 실정이다. 법원, 수사기관, 조사기관, 그리고 일반 기업을 포함하여 다양한 포렌식 관련 기관은 외부의 전문가를 채용하고 외부 자문위원을 위촉하며 내부의 포렌식 전문가를 다양한 외부 교육과정에 적극 참여시켜 디지털 포렌식을 위한 IT 기술에 대한 전문성을 더욱 높일 수 있도록 해야 한다.

□ 디지털 포렌식 전문 인력 양성 방안

국내 디지털 포렌식 전문 인력의 체계적이고 효과적인 양성을 위해서 크게 두가지의 방안을 소개한다. 첫번째, IT 분야별로 기술 능력이 인증된 전문인력을 중심으로 기초적인 포렌식 분야의 기술에 관하여 일정 기간 교육하여 인력을 양성하고, 국가기관이나 민간기관에서 필요시 인력 아웃소싱을 통하여 활용하는 방안이다. 이러한 방안은 수사기관이 아닌 제 3자에 의하여 증거를 수집함으로써 증거 수집에 대한 객관성을 높이고 증거의 변경 및 조작에 대한 시비를 좀 더 안전하게 방지할 수 있다는 장점이 있다. 두번째, 수사기관에서 증거 수집 활동을 한 경험자를 중심으로 디지털 포렌식 인력을 양성하는 방안이다. 이들은 포렌식의 기본 개념을 잘 알고 있는 반면, IT 전반적인 기술과 전문영역에 대한 이해가 부족하므로 IT 전문분야별 기술에 관하여 일정기간 교육하여 디지털 포렌식 전문가로 활동하도록 한다. 이러한 방안은 정예인력으로 포렌식 분야의 증거능력을 높일 수 있는 전문가의 양성이 가능하다는장점이 있다. 활발한 국내 IT 분야에서 전문 인력이 풍부하고 고부가가치 창출을 위한 새로운 솔루션에 대한 기대치가 높다는 관점에서 첫번째 인력양성 방안은 우수한 다수 인력의 활용이 가능하다는 점과 짧은 시간에 인력양성이 가능하다는 장점을 갖는다. 또한, 국내에서 수사기관의 증거에 대한 객관성이나 무결성에 대한 문제는 큰 약점일 수밖에 없었다. 이러한 문제를제 3자가 참여함으로써 좀 더 신뢰성과 객관성 있는 증거의 수집이 가능하고,해당 분야의 전문가의 활용을 통해 디지털 포렌식의 전문성을 한층 높을 수 있을 것이다. 그러나 포렌식 교육을 이수한 전문인력이라고 하더라도 수사기관의 특성을 이해하는데 어려움이 있을 수 있으므로 수사기관의 직원과 함께 작업하는 것이 바람직할 것이다. 두번째 IT 분야의 기초이론과 전문분야의 이론을 갖추기 위해서 최소한 3년에서 5년의 긴 시간이 필요하다는 단점을 갖는다. 또한, 지금까지 국내의 수사기관 종사자가많지 않다는 점도 근본적인 취약점이라고 할 수 있다. 그러나, 기존의 수사 경험을 기반으로 디지털 포렌식 수행 시 총체적 요구사항을 이해하고 있는 전문가가 다양한 IT 기술과 요소 기술에 대한 전문 지식을 배양함으로써 디지털 포렌식을 위한 수행 인력이 늘어나게 되고, 실제 관련 작업의 규모가 커질수록 이를 체계적으로 관리하여 효율성을 더욱 높일 수 있을 것이다.

5. 참고문헌

[1] 이형우, 이상진, 임종인, “컴퓨터 포렌식스 기술,” 정보보호학회지, 2002. 10
[2] 김종섭, 김귀남, “국내 Computer Forensics의 연구동향과 발전방향,” 정보보증논문지, 2003. 3
[3] 정덕영, “Windows 구조와 원리,” 한빛미디어, 2006.3.
[4] David A. Solomon and Mark E. Russinovich, "Inside Windows 2000, "Microsoft Press, 200.9.
[5] Brian Carrier, "File System Forensic Analysis," AD-dison-Wesley, 2005. 3
[6] National Software Reference Library (NSRL), http://www.nsrl.nist.gov
[7] Computer Forensic tool Testing (CFTT) Project, http://www.cftt.nist.gov