SeoulTech

7장 디지털 증거 분석 기술

박 종 혁 교수

UCS Lab

Tel: 970-6702

Email: jhpark1@seoultech.ac.kr

개요

- 학습 목표
  - 수집된 디지털 데이터를 분석하여 사건의 실마리 또는 증거를 찾기 위한 다양한 기술들을 살펴본다.
  - 디지털 증거 분석을 데이터 뷰잉, 검색, 통계 분석, 타임라인 분석 기술 등 다양한 기술에 대해 살펴본다.

- 학습 내용
  - 데이터 뷰잉, 디스크 브라우징 기술
  - 다양한 증거 분석 기술
  - 증거 분석 도구를 활용한 증거 분석
  - 안티 포렌식 대응 기술

목 차

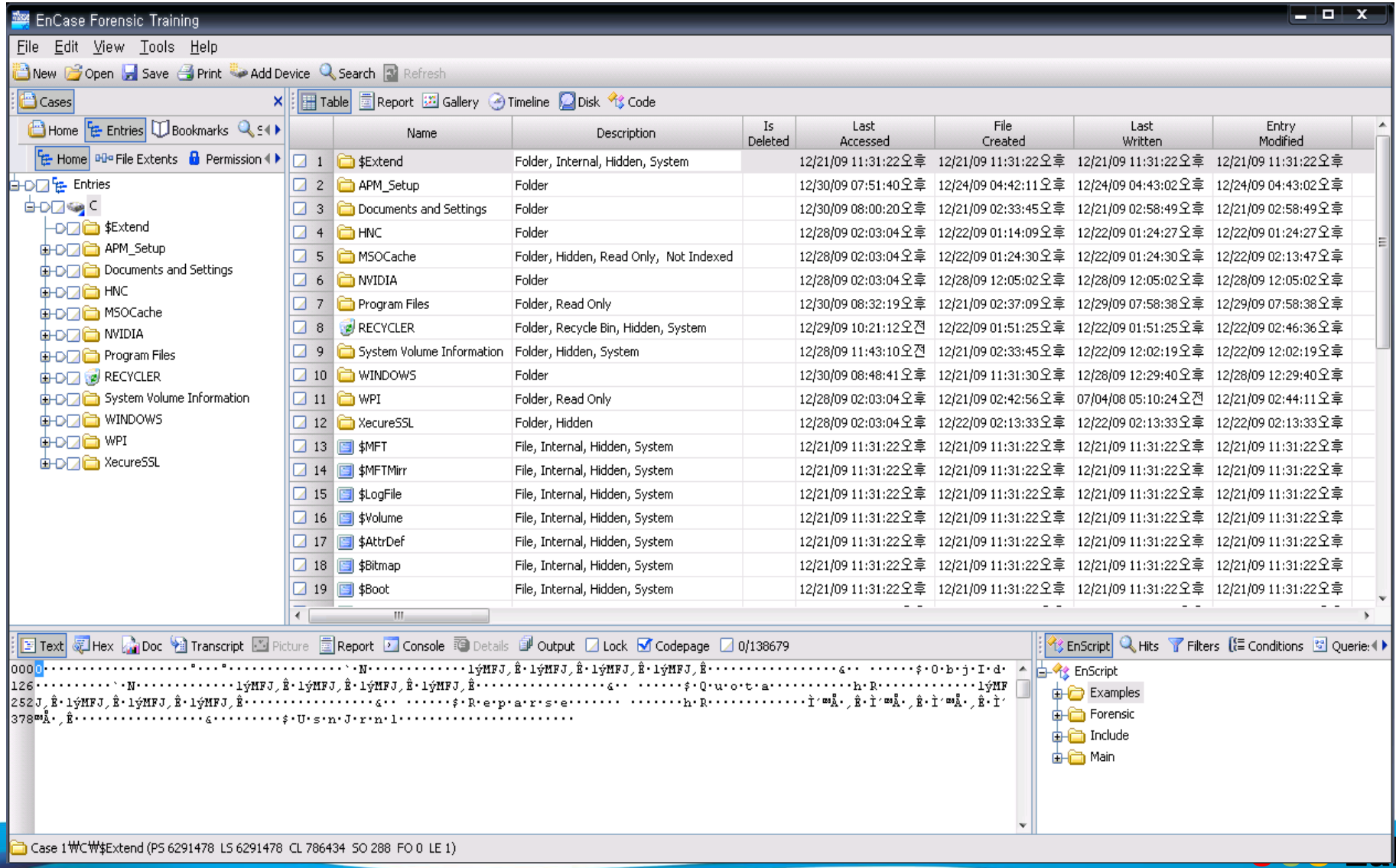
디스크 브라우징 기술

- 기본적인 증거 분석 대상은 확보한 저장 매체
  - 복제한 디스크 사본, 디스크 이미지 파일
  - USB 드라이브, CD 등의 저장 매체에서 생성한 이미지 파일

- 디스크 브라우징(Disk Browsing)
  - 저장매체 또는 하드디스크 이미지의 내부 구조와 파일 시스템을 확인하고, 파일시스템 내부에 존재하는 파일에 대응되는 응용 프로그램의 구동 없이 쉽고 빠르게 분석할 수 있도록 하는 기법
  - 복제한 이미지를 사용자가 수동으로 마운팅해서 열람할 필요가 없어 분석 시간을 줄일 수 있음
  - 디스크 브라우징 도구
    - EnCase, FTK, Final Forensic 등

디스크 브라우징 기술

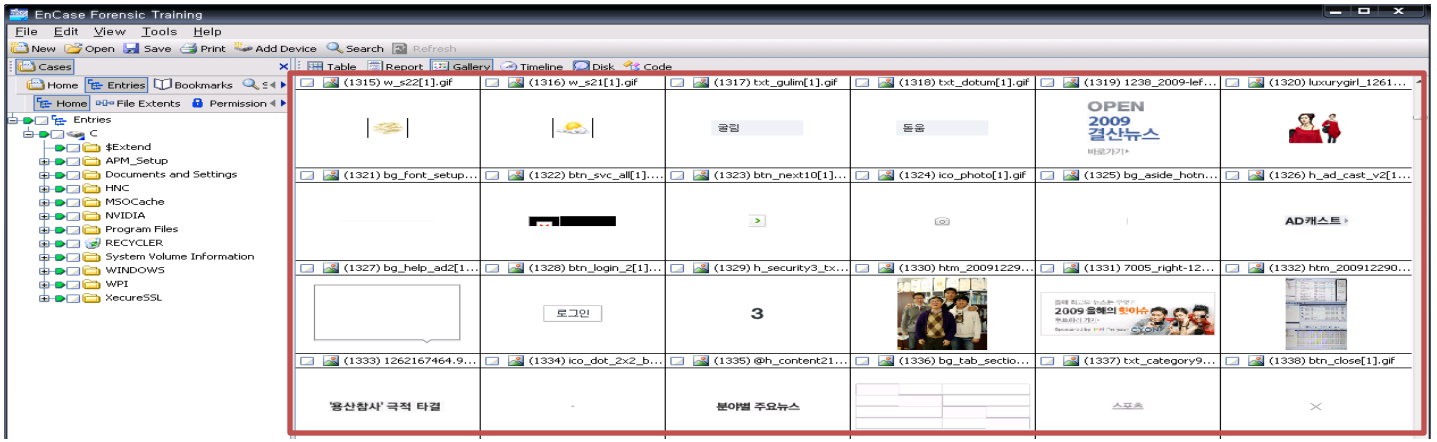
- **EnCase**의 디스크 브라우징 기능



EnCase의 디스크 브라우징

- 기본적인 디스크 브라우징 기능
  - 파일 시스템의 구조를 확인하고 메타데이터를 출력
  - 각 파일과 관련된 정보들 (생성 • 수정 • 접근 시간, 해쉬값, 시그니처, 저장 위치 등)을 파악
  - 검색, 타임라인 분석, 미리보기 기능 등

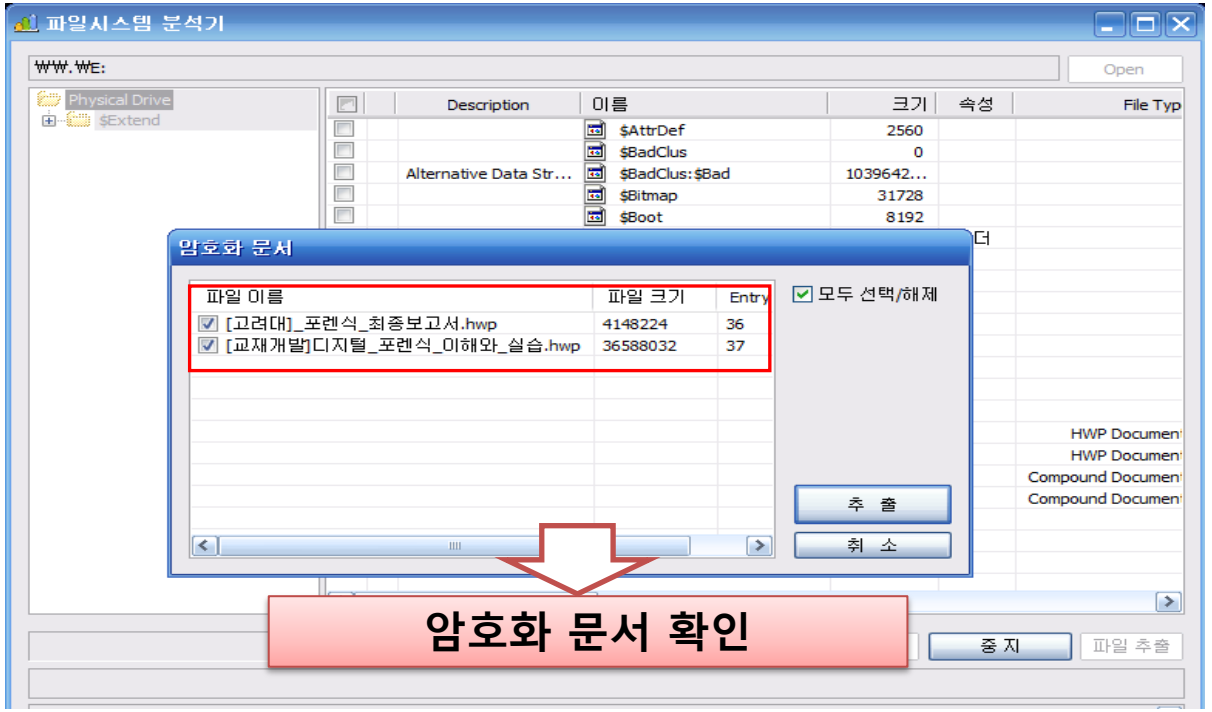
Name	Description	Is Deleted	Last Accessed	File Created	Last Written	Entry Modified
$Extend	Folder, Internal, Hidden, System		12/21/09 11:31:22오후	12/21/09 11:31:22오후	12/21/09 11:31:22오후	12/21/09 11:31:22오후
APM_Setup	Folder		12/30/09 07:51:40오후	12/24/09 04:42:11오후	12/24/09 04:43:02오후	12/24/09 04:43:02오후
Documents and Settings	Folder		12/30/09 08:00:20오후	12/21/09 02:33:45오후	12/21/09 02:58:49오후	12/21/09 02:58:49오후

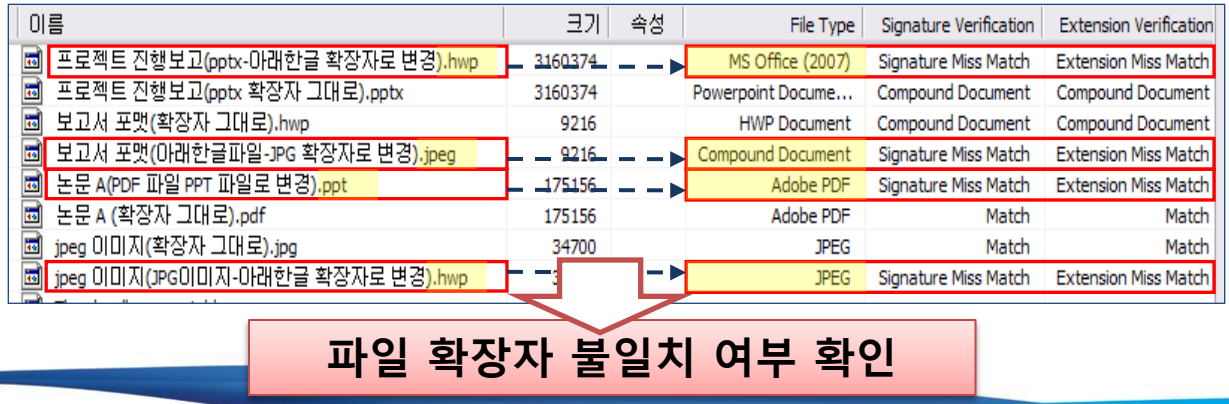


  - 파일 확장자 변경 여부, 암호 파일 등을 확인할 수 있으며, 복구 가능한 삭제 파일과 비할당 영역에 있는 파일 파편들을 검토

Miranda의 디스크 브라우징

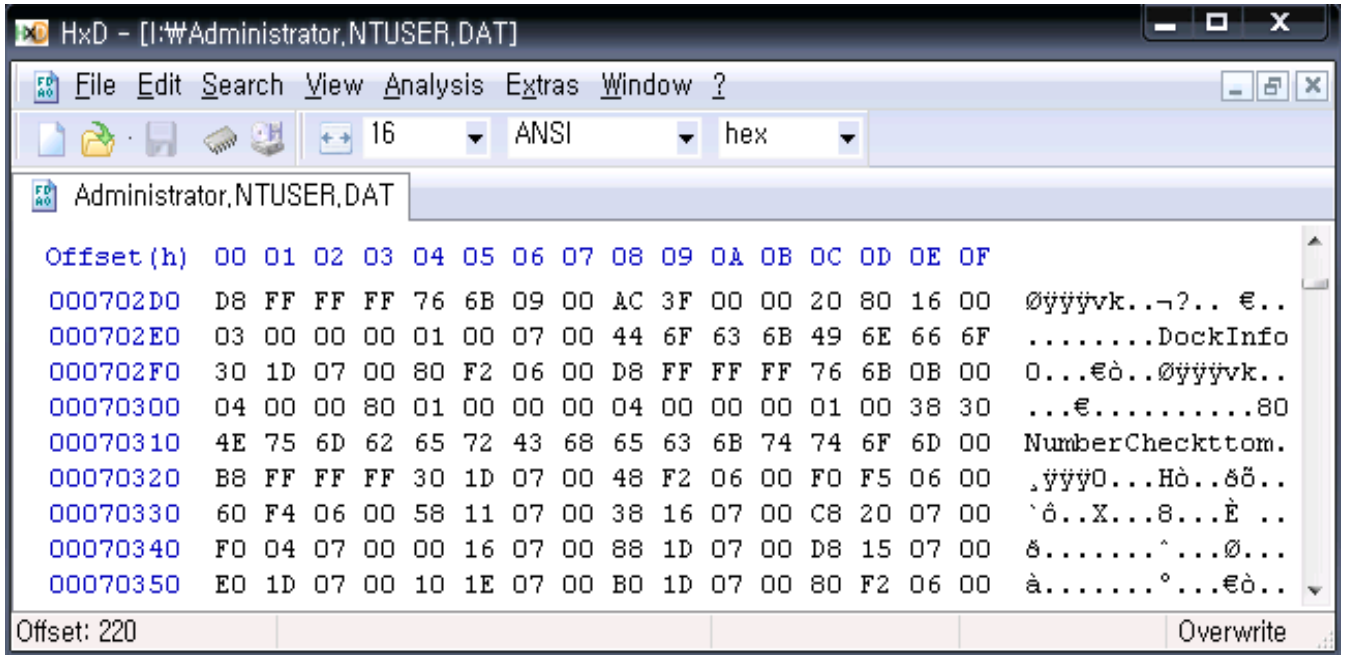
- Miranda 는 파일시스템 분석 도구로, 확장자를 변경한 파일 및 암호화 문서 파일 확인 가능





데이터 뷰잉 기술

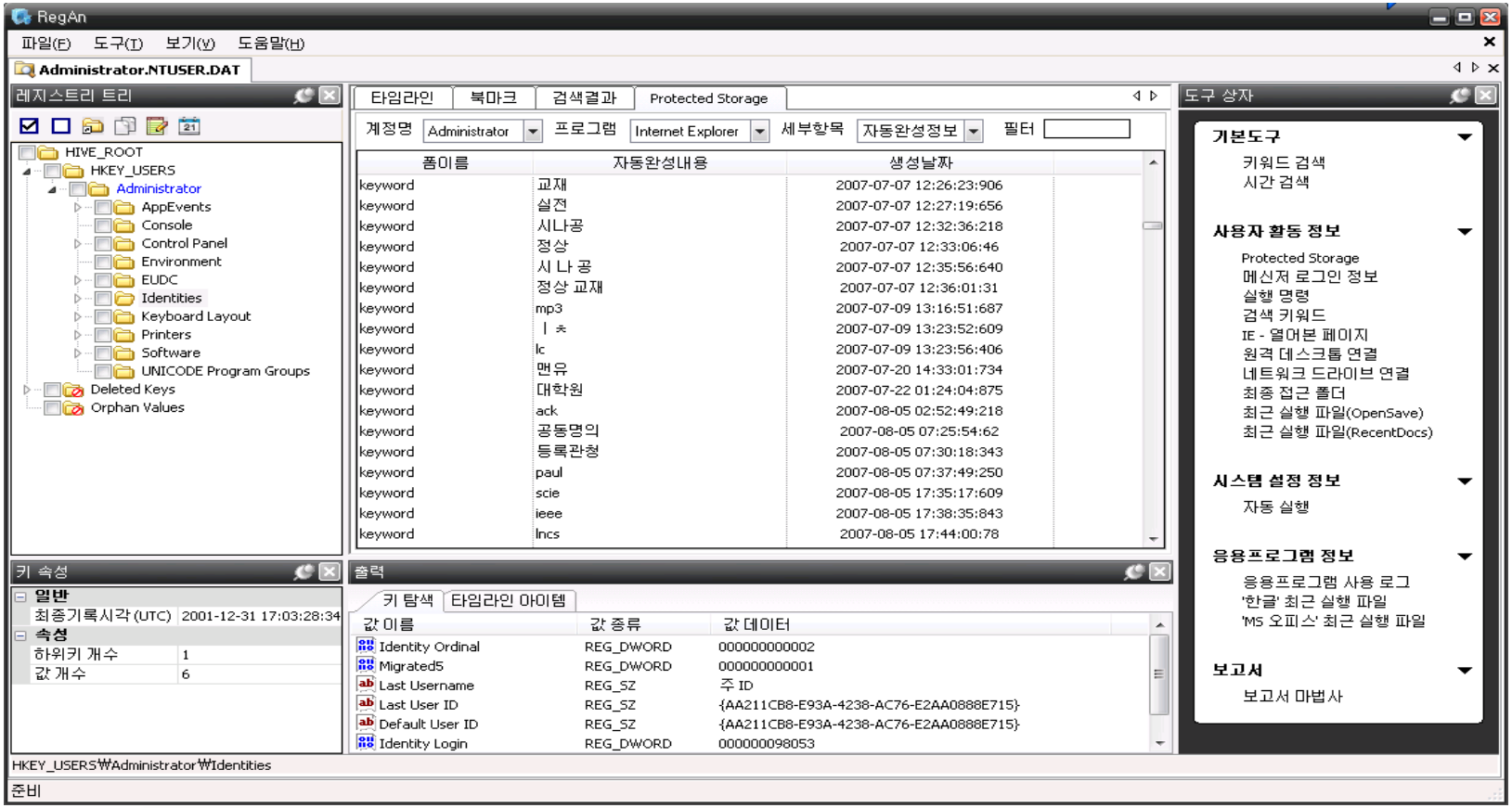
- 파일 포맷이 있는 데이터를 가시적으로 확인할 수 있도록, 디지털 데이터의 구조를 파악해서 시각적으로 정보를 출력하는 기술
- 헥스 에디터를 사용하기도 하지만, 좀더 효과적인 분석을 위해서는 개선된 데이터 뷰잉 기술이 필요



헥스 에디터(hex-editor)로 확인한 윈도우 레지스트리 파일

데이터 뷰잉 기술

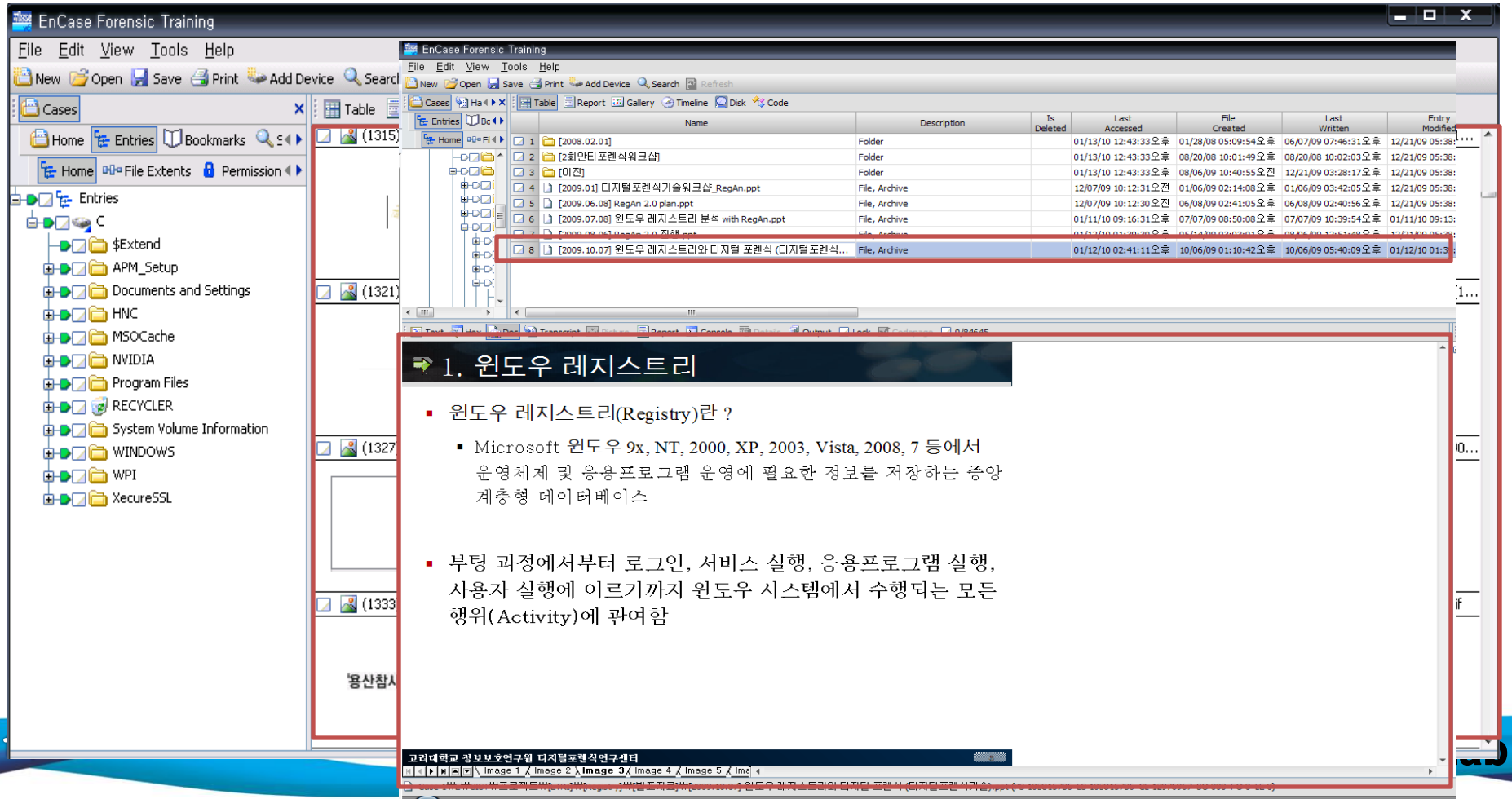
- **레지스트리 파일을 헥스 에디터(hex-editor)만으로 분석하기 힘든 단점을 보완하기 위해, 이를 가공해서** 사용자가 편리하게 분석할 수 있도록 도와주는 **RegAn**



RegAn: 윈도우 레지스트리 파일 뷰잉 & 분석 도구

데이터 뷰잉 기술

- 미리보기 기능
  - 문서, 사진 파일 등의 다양한 파일을 찾아낸 뒤, 개별적으로 응용프로그램을 실행하여 열람하지 않고 EnCase와 같은 도구로 한번에 볼 수 있도록 해주는 기능



검색 기술

- 검색 기술의 필요성
  - 저장매체가 대용량화 됨에 따라 수집되는 디지털 데이터의 양도 매우 많아지고 있어, 사건의 단서나 증거를 찾는 것은 점차 어려워짐
  - 사건과 관련된 자료들을 선별하기 위한 검색 기술 개발이 필요함

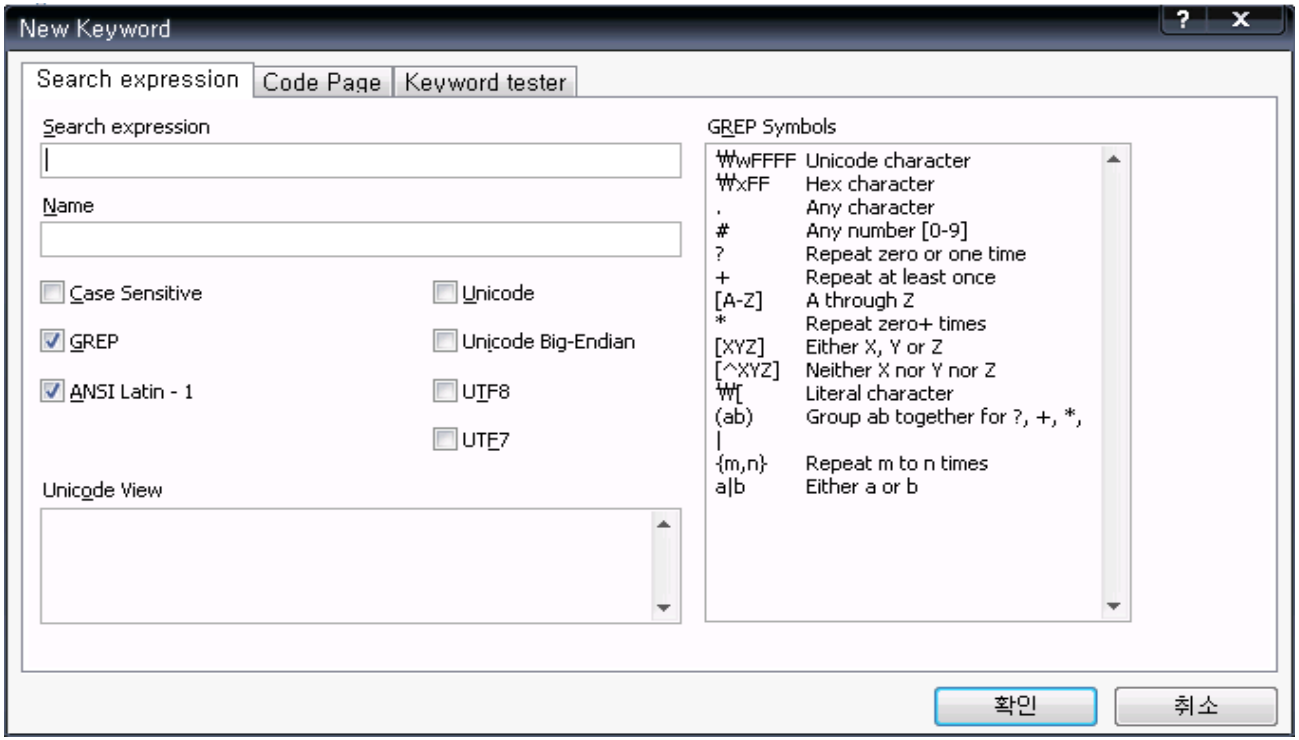
- 포렌식 조사/분석은 연속되는 검색의 반복
  - 모든 파일들의 키워드, Signature에 대해 검색을 반복해야 함
  - 잘 알려진 파일은 검색 대상에서 제외하고, 주목해서 검색할 대상을 선정하여, 검색 범위를 축소하는 것이 중요함.
  - 발전된 형태의 검색기술을 사용하여 조사/분석 단계에 투입되는 시간 비용을 줄일 수 있어야 함

검색 기술의 종류

- 일반 검색 (키워드 검색)
  - 파일 또는 저장매체 전체를 대상으로 특정 키워드를 입력하여 검색
  - 키워드 검색을 통해 필요한 증거를 찾기 위해서는 텍스트 인코딩, 대·소문자 등의 사항을 고려해야 함
  - 같은 키워드라도 인코딩 방식에 따라 전혀 다른 값이 되기 때문에 찾고자 하는 키워드의 형태를 결정해서 검색을 수행
  - 파일이름, 속성, 내부 문자열/코드값, 시그니쳐 등을 선정하여 목적 파일을 쉽고 빠르게 찾는 기술 (String, Index Search)
- 해쉬 검색
  - 기존에 구축된 알려진 파일의 해쉬 셋(Reference Data Set)을 사용하여, 조사 분석 대상을 식별하고 검색 수준을 선정할 수 있는 기술
- 슬랙 검색
  - 파일 시스템의 잉여 공간에 남아있는 기존 파일들의 조각 정보를 찾아내는 기술

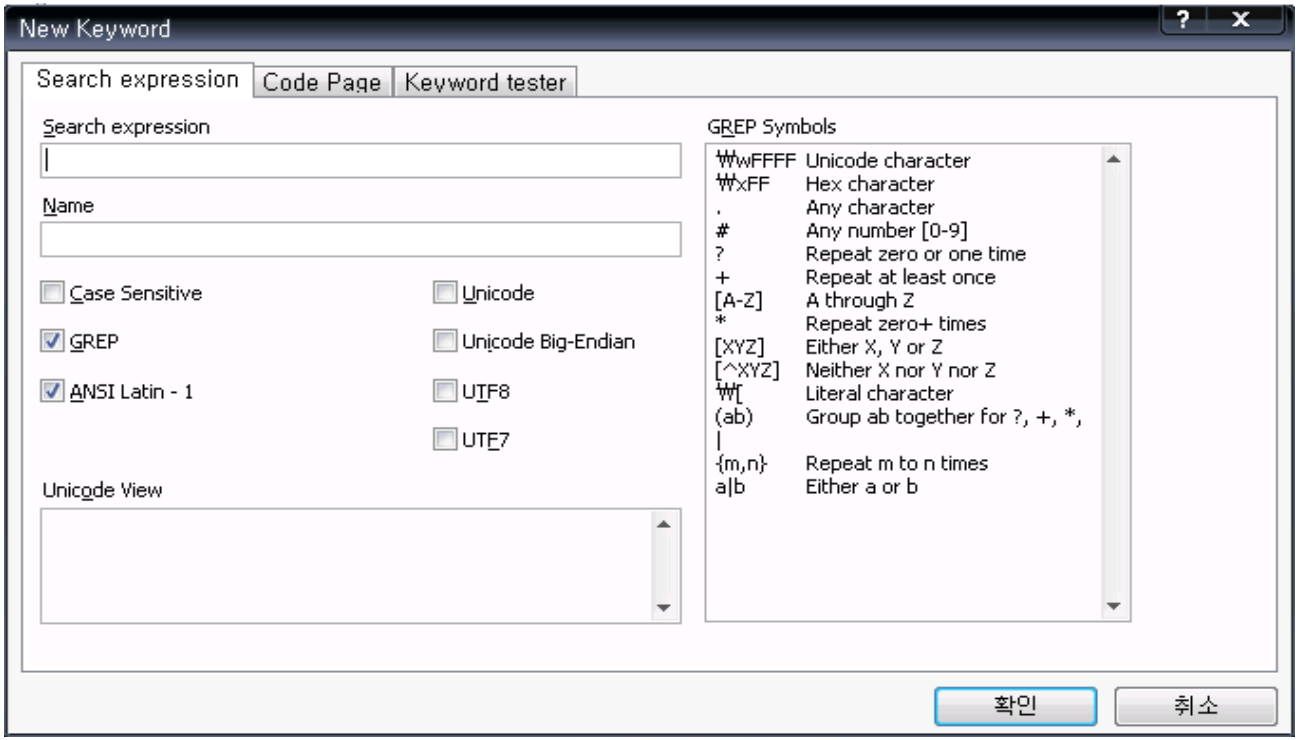
검색 기술 –키워드 검색

- **GREP(Globally Find Regular-Expression and Print)**
  - Unix 계열의 운영체제에서 검색을 위해 사용자가 정의할 수 있는 표현 명령어
  - 정규 표현식을 사용해서 다양한 형태의 키워드를 하나의 식으로 설정 가능



검색 기술 –키워드 검색

- **GREP(Globally Find Regular-Expression and Print)**
  - Unix 계열의 운영체제에서 검색을 위해 사용자가 정의할 수 있는 표현 명령어
  - 정규 표현식을 사용해서 다양한 형태의 키워드를 하나의 식으로 설정 가능



검색 기술 –키워드 검색

- **GREP(Globally Find Regular-Expression and Print)**

정규표현식	의 미	사용 예제
^	문자열의 처음	^aaa : 문자열의 처음에 aaa를 포함하면 매칭
$	문자열의 끝	aaa$: 문자열의 끝에 aaa를 포함하면 매칭
.	하나의 문자 매칭	.lue : alue, blue, clue ...
?	바로 이전 문자의 빈도가 0 또는 1인 경우 매칭	forensics? : forensic 또는 forensics
*	바로 이전 문자의 빈도가 0 이상인 경우 매칭	digital_*for : digitalfor, digital_for, digital__for ...
+	바로 이전 문자의 빈도가 1이상인 경우 매칭	digital_ + for : digital_for, digital__for ...
[ABC]	A, B, C 중의 하나의 문자 매칭	dig[ei]tal : digetal, digetal
[^ABC]	A, B, C 이외의 문자 매칭	dig[^i]tal : digetal, digftal ... (digital제외) [^a-z] : 소문자 이외의 문자 매칭
[A-C]	A부터 C중에 하나의 문자 매칭	[a-d] : a, b, c, d [0-2] : 0, 1, 2
₩	특수문자를 일반문자로 사용하는 경우	[?[₩]] : ?, [,]
X{M}	문자 X를 M번 반복	h{3} : h가 3번 이상 반복 (hhh, hhhh ...)
X{M,N}	문자 X를 M회 이상 N회 이하 반복	h{3,5} :hhh, hhhh, hhhhh
a|b	a, b 둘 중에 하나인 경우 매칭	web₩.(com)|(net) : web.com, web.net

검색 기술 –키워드 검색

- **GREP(Globally Find Regular-Expression and Print)**

Name	Kim	Number	870101-1234567
Name	Lee	Number	802110-2894561
Name	Park	Number	841218-1236874
Name	Han	Number	835577-1654789
Name	Hong	Number	880202-2345678

- 유닉스에서 **GREP** 명령어 사용하여 검색

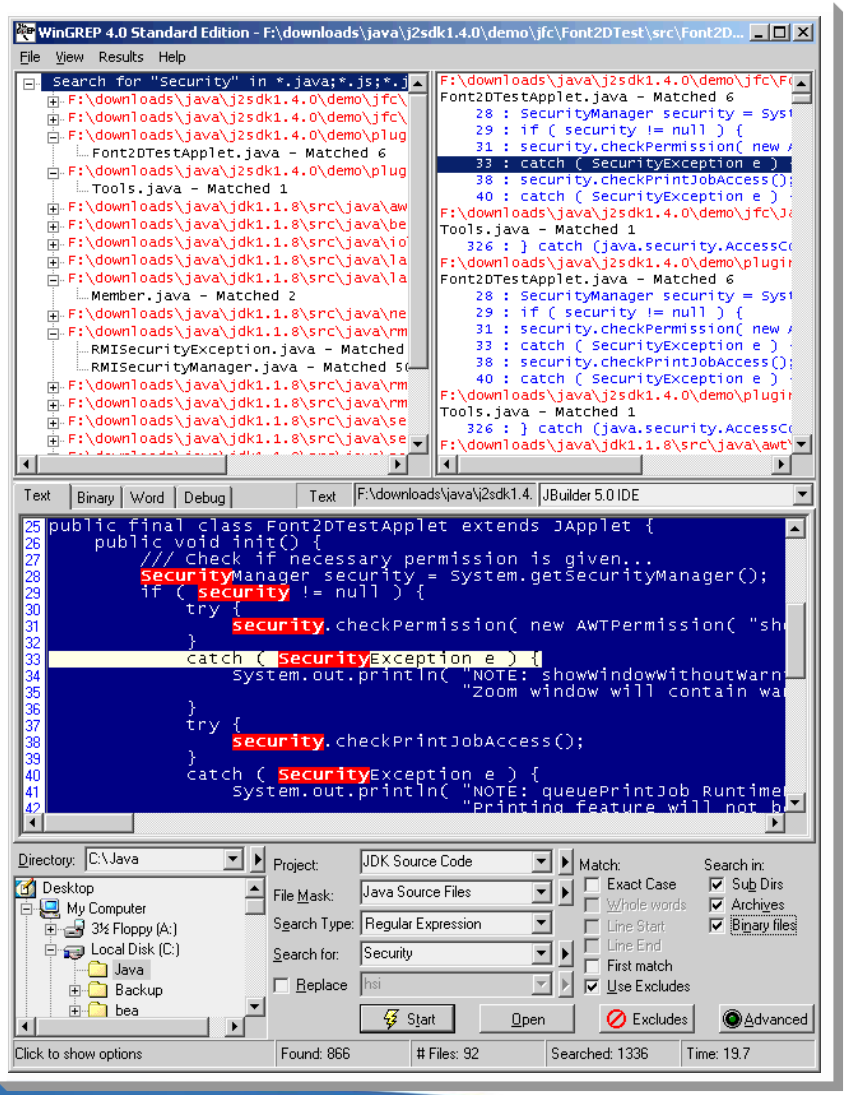
 # grep '.*[0-9]{2}[01]{1}[0-9]{1}[0-3]{1}[0-9]{1}-[0-9]{7}' DataFile

명령어 출력 결과

Name	Kim	Number	870101-1234567
Name	Park	Number	841218-1236874
Name	Hong	Number	880202-2345678

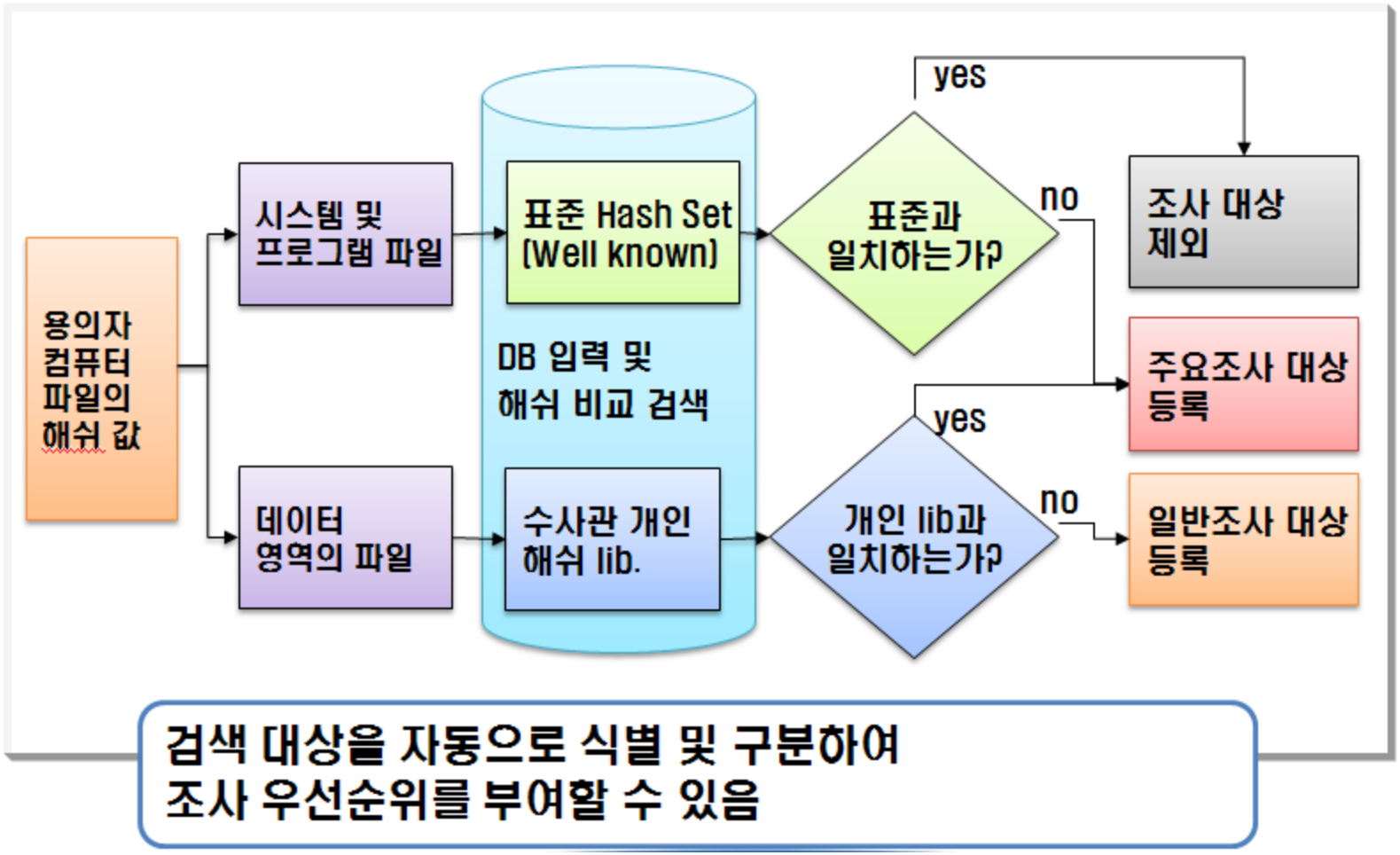
검색 기술–문자열 검색

- 파일 및 문자열 검색
  - 검색 작업은 지속적으로 이루어지므로 포렌식 전문 검색 도구를 쓰는 것이 유용함
  - WinGREP Search Tool (Hurricane Software)
    - 다중 디렉토리를 포함, 제외 검색
    - 키입력을 최소화한 사용자 인터페이스
    - 미리보기 기능
    - 압축/바이너리 파일에 대한 검색 기능
    - PDF/MS-Office 파일 검색 기능



검색 기술–파일 검색

- **Hashed Search 원리**



검색 기술 – 파일 검색

National Software Reference Library (NSRL)

- 美 NIST 산하 CFTT에서 제공하는 국가 표준 참조 데이터
- Justice's National Institute of Justice (NIJ)의 지원
- NSRL의 목적
  - 범죄에 사용되는 컴퓨터 파일의 식별 자동화
  - 증거에 포함된 파일 조사를 효율적으로 지원
- NSRL의 세부 내용
  - 다년간 각종 S/W 및 알려진 파일을 수집, 이에 대한 정보와 hash 값을 DB 목록화 (TOTAL 50,121,818 files, 15,722,076 unique hash values)
  - 전세계 8천여 개 S/W, 35개국 언어 OS의 참조 데이터 셋(RDS:Reference Data Set) 구축

```
"SHA-1",                                    "MD5",                                  "CRC32",   "FileName",       "FileSize","ProductCode"
"00000F6ED90D946C057B55545597C3125lDC24E4","F4l29AC77F806601BDD44620Cl7675E7","38CC50B7","004i200r.gif"   ,  1551,228,    "WIN"
"00000FF9D0ED9A6B53BC6A9364C07074DE1565F3","A5D49D6DA9D78FD1E7C32D58BC7A46FB","2D729AlE","cmnres.pdb.dll",76800,2471,    "WIN"
"00000FF9D0ED9A6B53BC6A9364C07074DE1565F3","A5D49D6DA9D78FD1E7C32D58BC7A46FB","2D729AlE","cmnres.pdb.dll",76800,2704,    "WIN"
"00000FF9D0ED9A6B53BC6A9364C07074DE1565F3","A5D49D6DA9D78FD1E7C32D58BC7A46FB","2D729AlE","cmnres.pdb.dll",76800,2741,    "WIN"
"00000FF9D0ED9A6B53BC6A9364C07074DE1565F3","A5D49D6DA9D78FD1E7C32D58BC7A46FB","2D729AlE","cmnres.pdb.dll",76800,2797,    "WIN"
"00000FF9D0ED9A6B53BC6A9364C07074DE1565F3","A5D49D6DA9D78FD1E7C32D58BC7A46FB","2D729AlE","cmnres.pdb.dll",76800,2912,    "WIN"
```

검색 기술–파일 검색

NSRL 활용방안

- 용의자 컴퓨터내의 파일내용과 NSRL 목록을 비교 분석, 알려진 파일을 쉽게 식별하여 조사 범위 집중 가능
- 수사관은 평소 표준 참조 데이터를 입수하거나 제작하여 분석·조사 과정을 효율적으로 체계화하여야 함

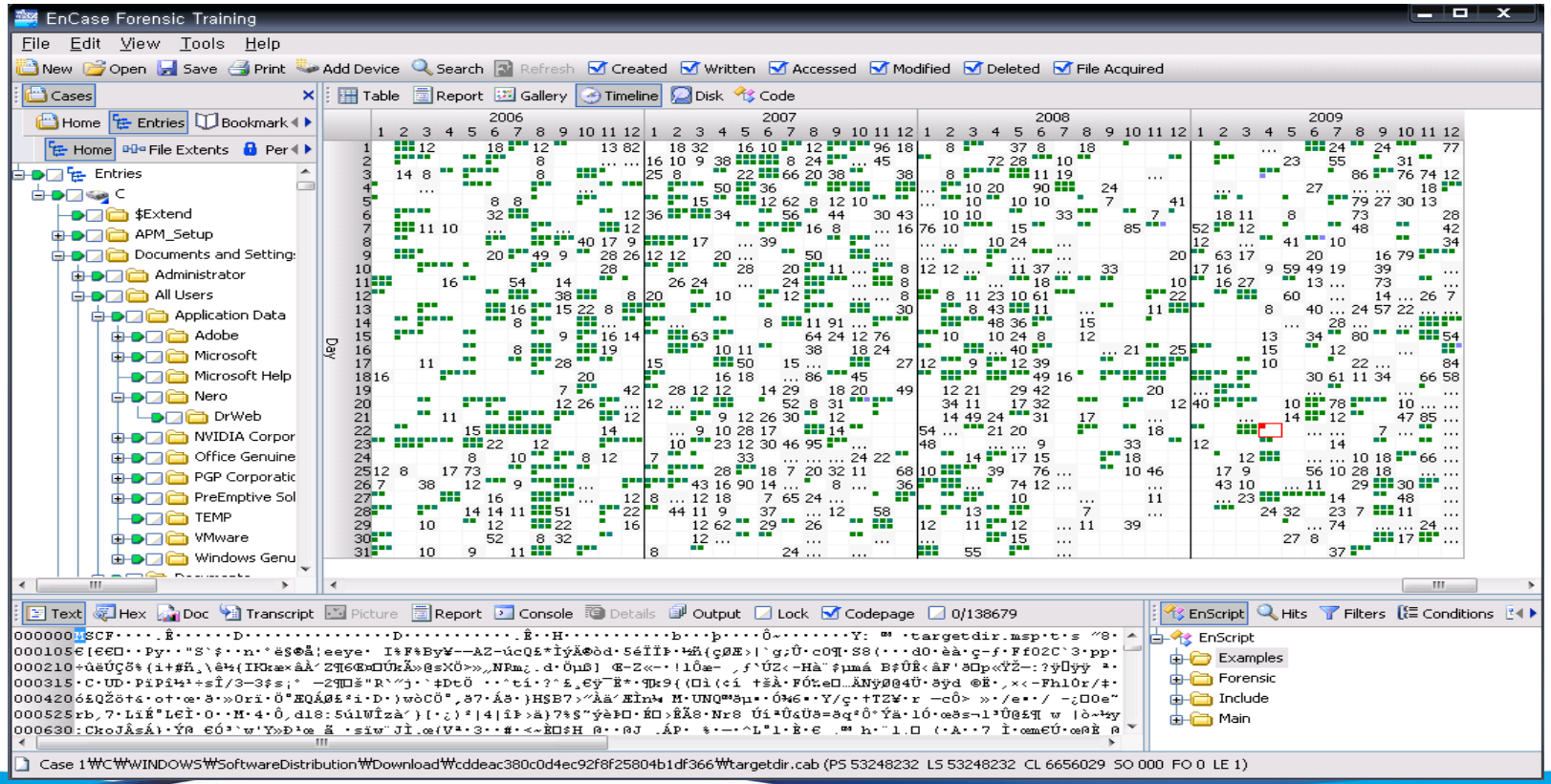
인덱스 기반 검색 기술

- 새로운 검색 기술의 필요성
  - 데이터의 대용량화
    - 하드디스크 기술 발달로 S-ATA 1TB까지 시판
    - 문서, 그림, 동영상의 다양한 데이터를 인터넷으로 공유함으로써 조사에 필요한 데이터 량이 크게 증가
    - OS와 응용 프로그램의 크기 증가 등
  - 소요 시간의 증가
    - 대용량 데이터를 수집하고 분석하는데 많은 시간이 소요됨
    - 컴퓨터 처리 속도 증가에 비해 처리할 데이터는 엄청나게 증가함

- 해결 방안
  - 디스크 이미지에 대한 인덱스를 생성하여 데이터를 빠르게 검색

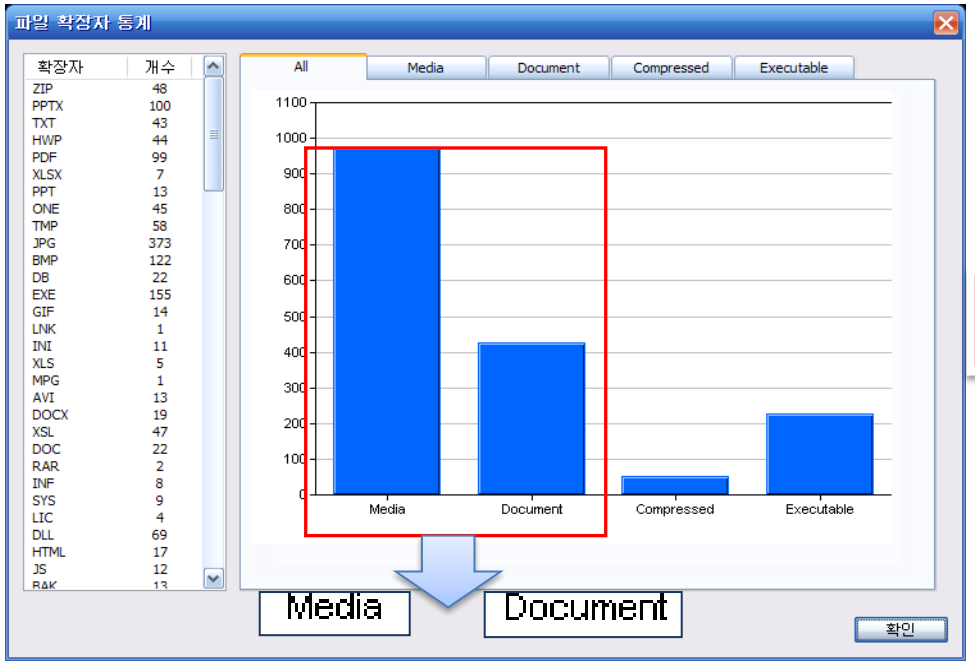
타임라인 분석

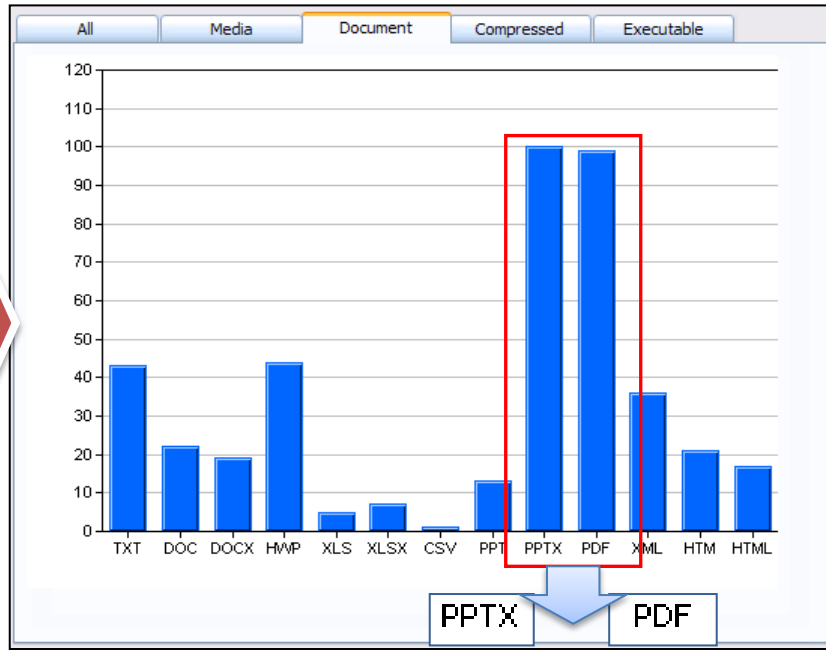
- 타임라인 분석
  - 디지털 데이터의 시간 정보는 범죄 사실을 규명하기 위해 매우 중요한 정보
  - 파일 시스템 상에 저장되는 파일의 시간 정보, 파일 내부의 메타데이터에 저장되는 시간 정보 등 다양한 곳에 저장되어 있는 시간 정보를 이용,타임라인(Timeline)을 구성함으로써 시스템 사용자의 행위를 추적할 수 있음



통계 분석

- 통계 분석
  - 파일 종류 별 통계 분석으로 사용자의 컴퓨터 사용 수준을 파악할 수 있으며 시스템의 주요 사용 목적을 추측할 수 있음
  - 아래 Miranda의 파일 별 통계 분석으로, 현재 파일 시스템에는 멀티미디어(화상, 동영상 등)와 문서 파일이 많이 존재한다는 것을 확인할 수 있음





로그 분석

- 로그(LOG)란?
  - 시스템에 접속한 사용자의 행위 및 시스템의 상태를 주기적으로 저장해 놓은 기록
  - 로그를 이용하여 외부 침입의 흔적과 사용자가 어떠한 명령어를 사용했는지, 그리고 시스템이 처리한 업무와 에러 등의 정보 등을 파악
  - 서버 시스템의 침해사고조사와 같은 경우 가장 기본적으로 행해지는 분석 중의 하나

- 로그의 종류
  - Unix 시스템 계열 로그, Windows 계열 로그, 웹(Web) 로그 등
  - 시스템의 종류에 따라 특별한 설정 없이 기본적으로 생성되는 로그가 있는 반면, 사용자의 설정이 있어야만 생성되는 로그도 존재
  - 조사자는 각 시스템의 기본 로그와 그렇지 않은 로그의 분석 방법을 숙지해야 함

로그분석 – Unix 시스템 로그 분석

- 시스템 별 로그 디렉터리

Unix 시스템	디렉터리
HP-UX	/usr/adm
Solaris, AIX	/var/adm
Linux, BSD	/var/log

- 로그 파일의 종류 및 기본적인 기능

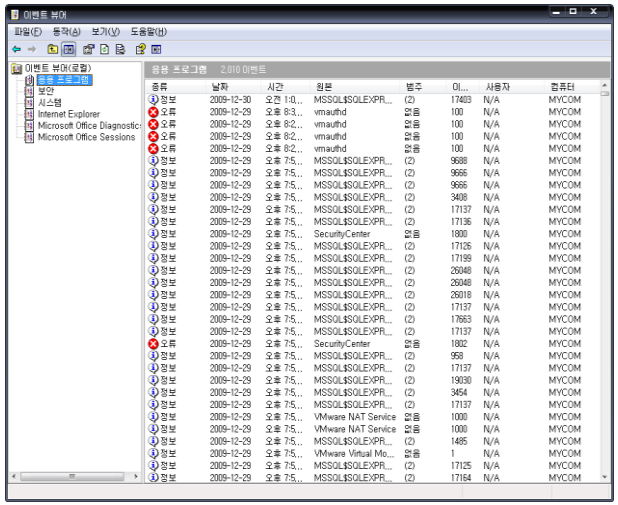
파 일 명	기 능
acct 또는 pacct	사용자별로 실행되는 모든 명령어를 기록
aculog	다이얼-아웃 모뎀 관련 기록(자동 호출 장치)
lastlog	각 사용자의 가장 최근 로그인 시간을 기록
loginlog	실패한 로그인 시도를 기록
messages	부트 메시지 등 시스템의 콘솔에서 출력된 결과를 기록하고 syslog에 의하여 생성된 메시지도 기록
sulog	su 명령 사용 내역 기록
utmp	현재 로그인한 각 사용자의 기록
utmpx	utmp 기능을 확장(extended utmp), 원격 호스트 관련 정보 등 자료 구조 확장
wtmp	사용자의 로그인, 로그아웃 시간과 시스템의 종료 시간, 시스템 시작 시간 등을 기록
wtmpx	wtmp 기능 확장 (extended wtmp)
vold.log	플로피 디스크나 CD-ROM과 같은 외부 매체의 사용에서 발생하는 에러를 기록
xferlog	FTP 접근 기록

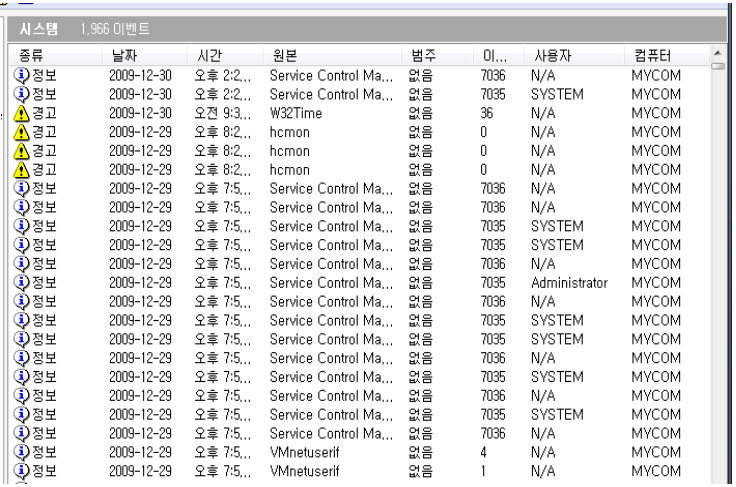
로그분석 – Windows 시스템 로그 분석

- 이벤트 로그
  - Windows는 기본적으로 이벤트(event) 로그를 시스템 운영 전반에 걸쳐서 저장
  - 조사자는 이벤트 로그의 분석을 통해 해당 시스템의 전반적인 동작을 알 수 있으며, 증거 자료를 획득할 수도 있음

- 이벤트 로그의 종류
  - 응용프로그램 로그
    - 응용프로그램이나 기타 프로그램의 동작에 대한 이벤트가 저장되며, 기록되는 이벤트는 소프트웨어 개발자에 의해 결정
  - 보안 로그
    - 유효하거나 유효하지 않은 로그온 시도 및 파일 생성, 열람, 삭제 등에 관련된 이벤트를 기록
  - 시스템 로그
    - Windows 시스템 구성요소가 기록하는 이벤트로 시스템 부팅 시 드라이버가 로드되지 않는 경우와 같이 구성요소의 오류를 기록

로그분석 – Windows 시스템 로그 분석





이벤트 헤더 정보

정 보	의 미
날 짜	이벤트가 발생한 날짜
시 간	이벤트가 발생한 시간
사 용 자	이벤트를 발생시킨 사용자의 이름
컴 퓨 터	이벤트가 발생한 컴퓨터의 이름
원 본	이벤트를 기록한 소프트웨어 (이벤트가 일어난 프로세스)
이벤트ID	해당 원본의 특정 이벤트 유형을 식별하는 번호
범 주	이벤트의 원본에 의한 이벤트 분류로 주로 보안 로그에서 사용됨
종 류	이벤트 심각도의 분류로 오류, 정보, 경고, 성공, 감사, 실패 감사로 분류

이벤트 정보의 종류

이벤트 유형	설 명
오 류	데이터 손실이나 기능 상실 같은 중대한 문제로 시스템을 시작하는 동안 서비스가 로드되지 못했을 경우와 같은 이벤트 기록
경 고	시스템에 문제가 발생할 수 있는 문제를 미리 알려 주는 이벤트로 디스크 공간이 부족할 때와 같은 이벤트 기록
정 보	응용 프로그램, 드라이버 또는 서비스가 성공적으로 수행되었음을 설명하는 이벤트
성공감사	사용자가 시스템에 성공적으로 로그온 했을 경우와 같이 보안 이벤트가 성공했음을 나타냄
실패감사	사용자가 시스템에 로그온 실패했을 경우와 같이 보안 이벤트가 실패했음을 나타냄

로그분석 – Web 로그 분석

- 웹 서비스를 제공하는 웹 서버의 종류에 따라 다른 형태로 저장

- **CLF(Common Log Format)**로 파일을 생성, 웹 서버의 종류와 설정에 따라 조금씩 차이

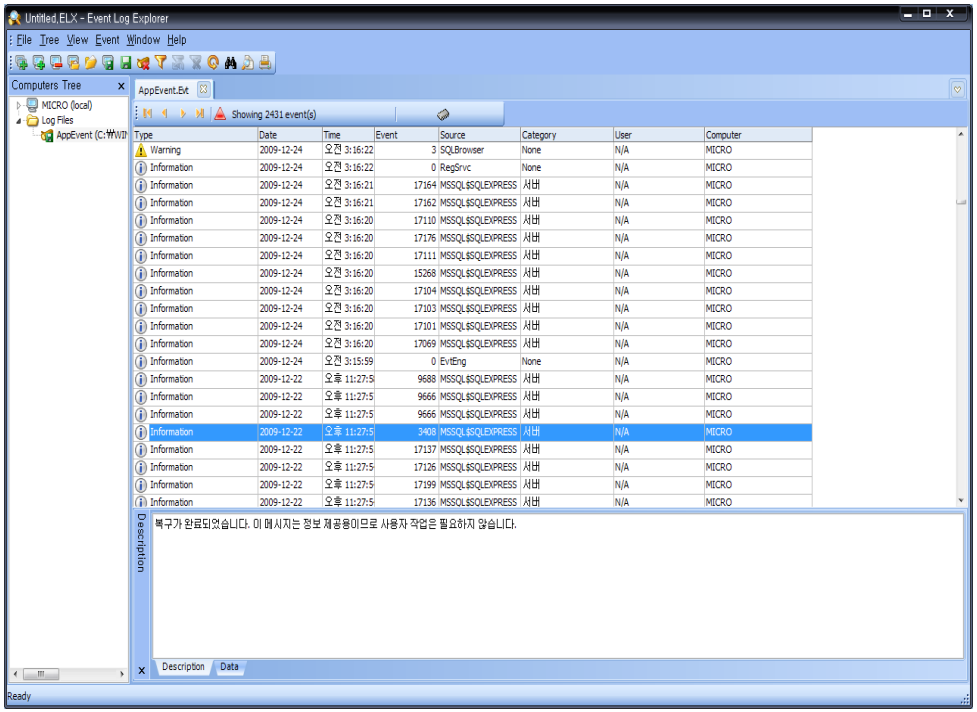
CLF 저장 정보 및 설명

로그 정보	설 명
Host	클라이언트의 호스트 이름이나 IP 주소
Authuser	인증이 필요한 경우 사용자 이름 기록
Date	접속한 시간과 날짜 기록
Request	클라이언트가 요청한 메시지
Status	요청한 것에 대한 서버의 처리사항 (상태 코드)
Bytes	전송된 Bytes의 크기 (헤더 제외)

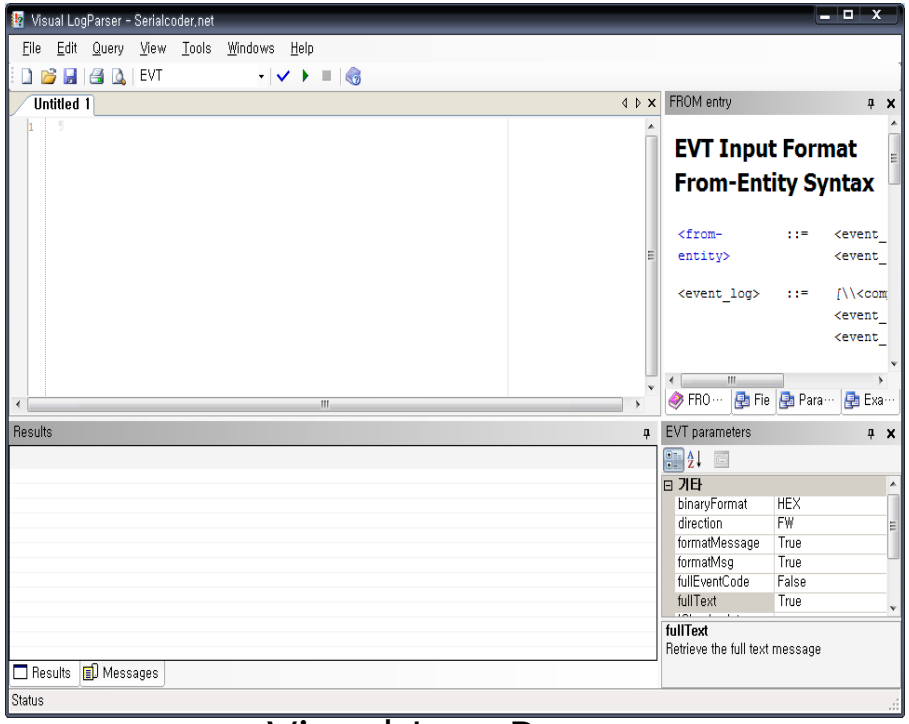
로그분석 – 로그 분석 도구

- **Event Log Explorer**
  - ➢ 로그에 대한 부가 설명 및 바이너리 데이터 제공

- **Log Parser**
  - ➢ 커맨드 라인에서 실행, 텍스트 기반의 로그를 SQL 쿼리를 이용하여 분석



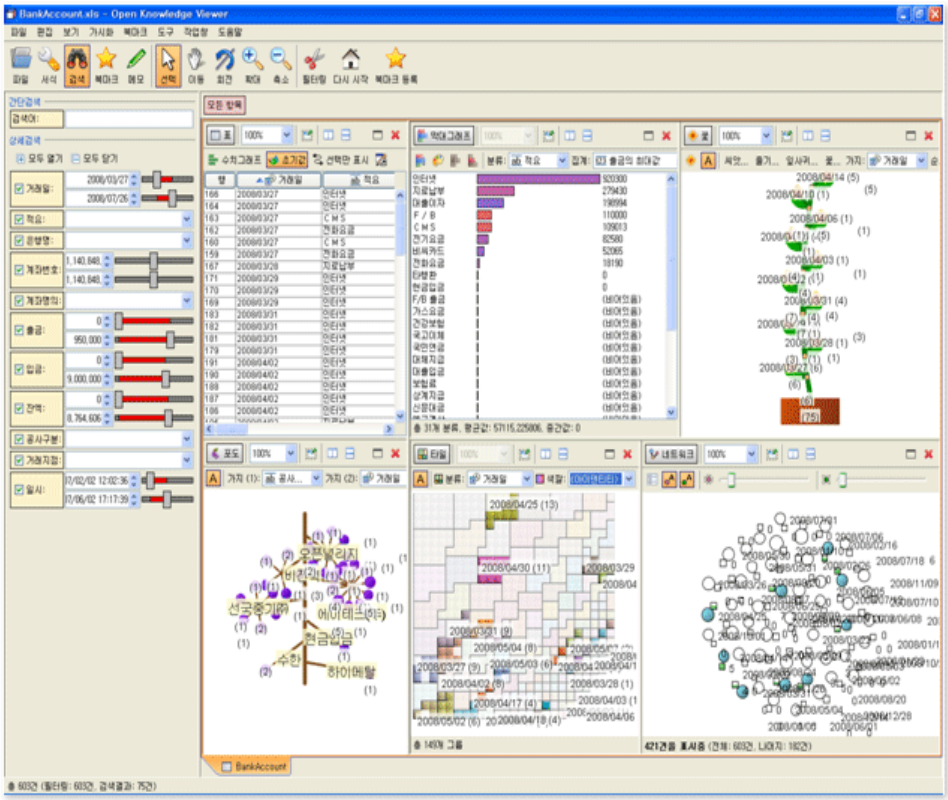
Event Log Explorer



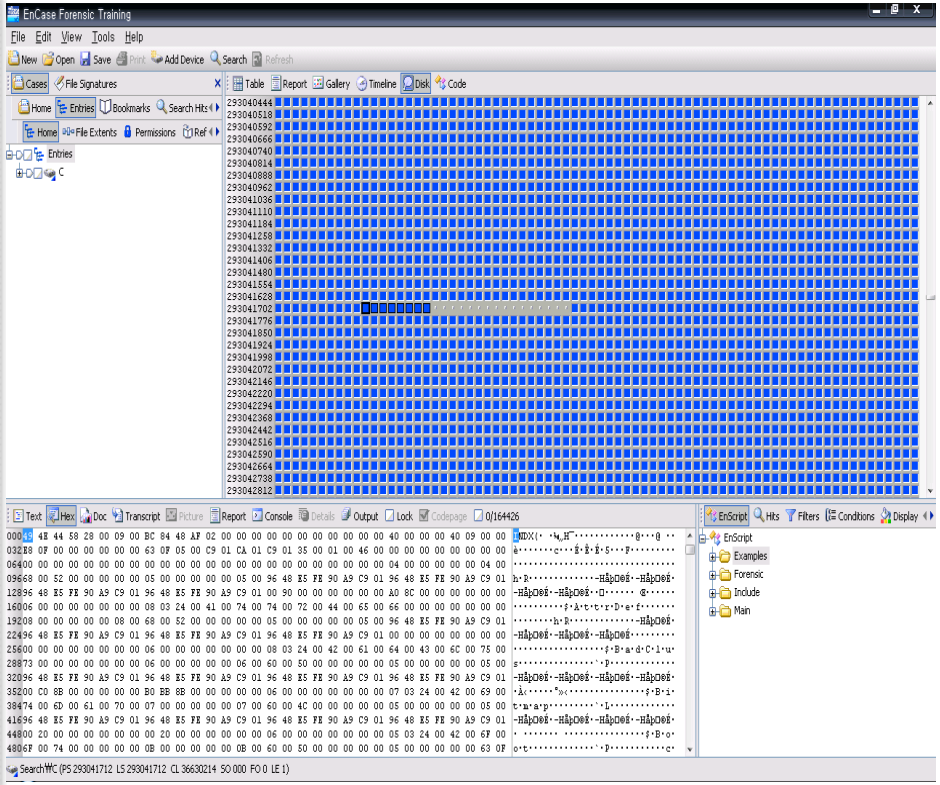
Visual Log Parser

시각화 기술

- 보이지 않는 것을 일정한 형태로 나타내거나 가려져 있던 어떤 현상이나 실체가 눈에 띄게 드러나게 하는 것으로 추상적인 자료를 사람이 인지할 수 있는 형대로 만드는 과정



Open Knowledge Viewer

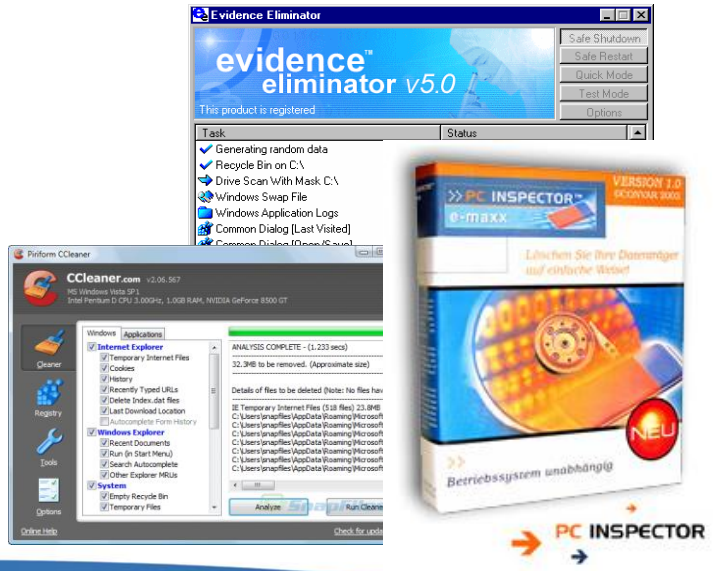


EnCase의 디스크 할당 상태 시각화 기능

안티 포렌식 대응 기술

- 안티 포렌식 **(Anti-Forensic)**이란?
  - 포렌식 기술에 대응하여 자신에게 불리하게 작용할 가능성이 있는 증거물을 차단하려는 일련의 활동
  - 과거에는 증거가 될 수 있는 자료들을 수동으로 처리하였지만, 최근에는 추적 및 증거물 획득을 원천적이고 자동화된 방법으로 막아주는 전문 제품들이 등장하고 있음

- 안티 포렌식 기법
  - 주로 데이터 암호화 등을 통한 복구 기법 회피, 중요 증거 데이터의 증거 자동 삭제, 데이터 은닉 제품 등이 있음
  - 데이터 영구 삭제
    - Disk Wiping, Degausser
    - 증거 자동 삭제
  - 데이터 암호화
    - 압축파일, 문서파일 등의 암호화 등
  - 데이터 은닉
    - 스테가노그래피



안티 포렌식 대응 기술 – 데이터 영구 삭제

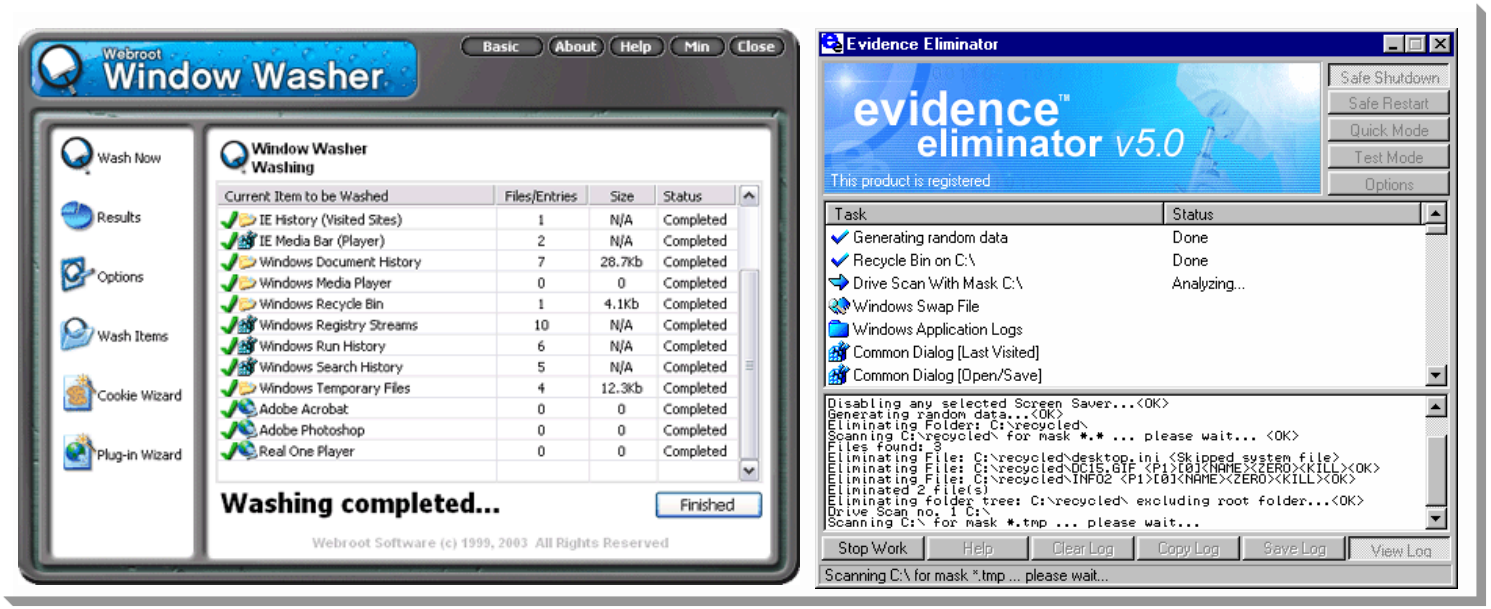
- **Disk Wipe**
  - 하드디스크의 기존 데이터를 완벽히 제거하고 모든 Sector의 내용을 0으로 만드는 과정
- 디가우저 (소자, **Degausser**)
  - 하드디스크나 테이프에 강력한 자기장을 노출시켜 기록된 데이터를 파괴하고 복구가 불가능하도록 하는 장비

[Disk Wipe S/W]


소자용 전문 제품
(Degausser – BTE)

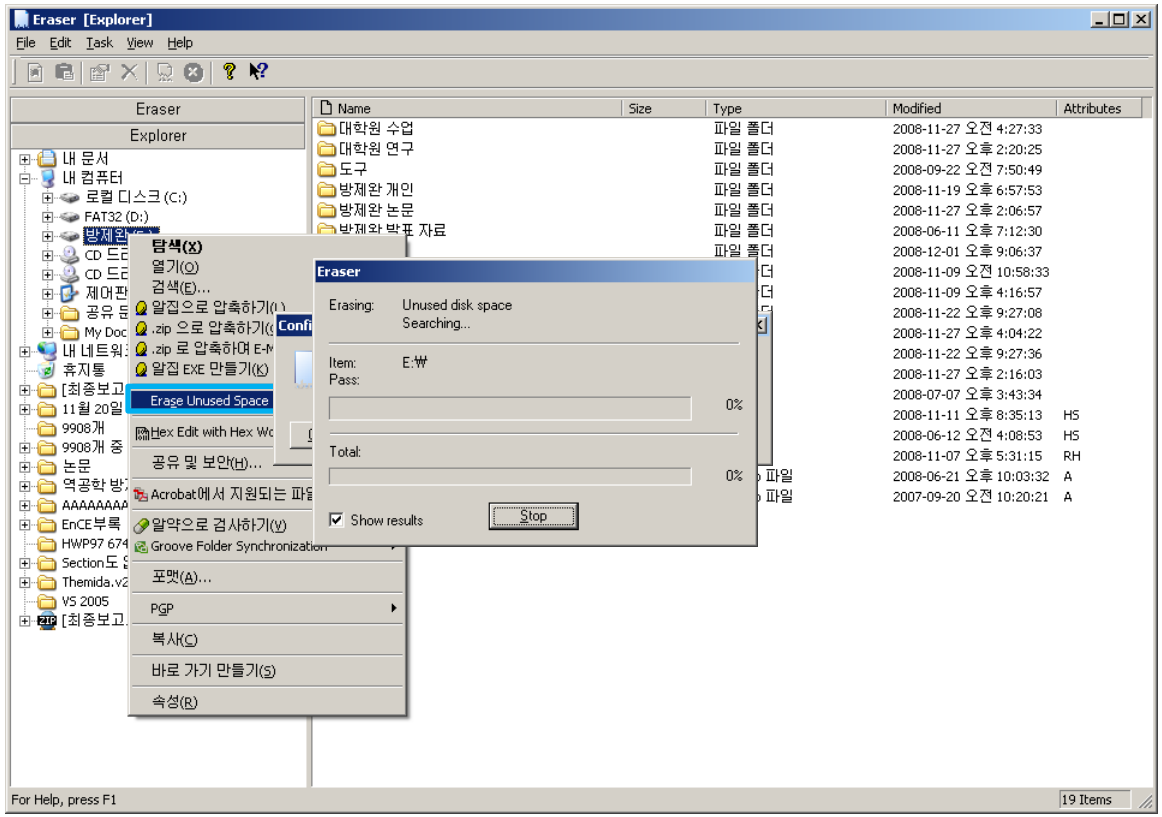
안티 포렌식 대응 기술 – 데이터 영구 삭제

- 증거물 생성의 사전 봉쇄
  - 목적 : OS에서 자동으로 생성되는 정보 중,
    증거가 될만한 모든 정보들을 생성하는 즉시 자동으로 삭제
  - 특징 : Web Pages, 그림, 동영상, 음성파일, E-mail,
    레지스트리, 쿠키, 히스토리 파일등이 주요 삭제 대상
  - 제품 : Window Washer, Evidence Eliminator 등



안티 포렌식 대응 기술 – 데이터 영구 삭제

- **Eraser** 디스크 미사용 영역 완전 삭제



안티 포렌식 대응 기술 – 데이터 영구 삭제

- 데이터 복구 기법 회피 기술
  - 디스크 덮어쓰기
    - 삭제된 파일의 데이터 중 물리적으로 디스크에 남아있는 부분을 덮어쓰고 삭제하는 과정을 반복하면 데이터 복구 기법을 회피할 수 있음
    - 美 국방성(DoD)에서는 기밀 자료를 삭제하기 위한 표준 (DoD5220, 22-M)을 다음과 같이 제시하고 있음

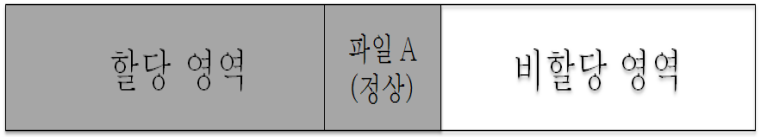
      1. 임의의 문자로 데이터를 덮어 씀
      2. 첫 번째 문자의 보수로 덮어씀
      3. 다시 임의의 문자로 데이터를 덮어씀
      4. 이 과정을 7회 반복

안티 포렌식 대응 기술 – 데이터 영구 삭제

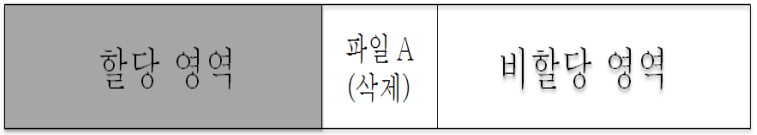
- 데이터 복구 기법 회피 기술 (계속)
  - Final eRaser
    - 제조사 : 한국 Final data社
    - 목적 : 자신의 하드 디스크에 저장되어 있는 자료를 파일, 디렉토리, 디스크 단위로 완벽하게 삭제
    - 특징 : 미 국방성 권고안(DoD5220, 22-M)인 7회 삭제보다 더 강화된 수준으로 36회 덮어쓰기 및 삭제를 반복
    - 이러한 삭제방법은 S/W적인 방법 이외에도 H/W적인 방법으로도 복구가 불가능 함

안티 포렌식 대응 기술 – 데이터 복구

- 데이터 복구는 저장 매체의 비 할당 영역으로부터 삭제된 데이터를 복구하는 기술



하드 디스크의 추상적인 구조 : 파일 A(정상)



하드 디스크의 추상적인 구조 : 파일 A(삭제)

- 파일 A를 삭제하면 데이터가 그대로 유지된 채 비 할당 영역으로 들어가게 된다. 삭제된 파일은 파일 시스템의 비 할당 영역에 잔존

- 데이터는 새로운 파일 생성되어 해당 영역이 덮어 씌워지지 않으면 데이터 복구 도구를 이용하여 복구 가능

안티 포렌식 대응 기술 – 데이터 복구

삭제 파일 복구 기술의 필요성

- 비할당 영역에서 삭제 파일을 복구함으로써 심도 있는 컴퓨터 사용 흔적 조사가 가능
- 용의자 및 범죄자는 증거 인멸을 위해 저장 매체를 물리적으로 파괴, 훼손하거나 디지털 증거를 삭제할 가능성이 높으므로, 이를 원래의 상태로 복구하는 기술이 필요함

파일시스템의 영역

- **메타데이터 영역** : 파일의 이름, 만든이, 날짜, 크기 등을 저장
- **데이터 영역** : 파일의 실제 데이터 스트림 저장

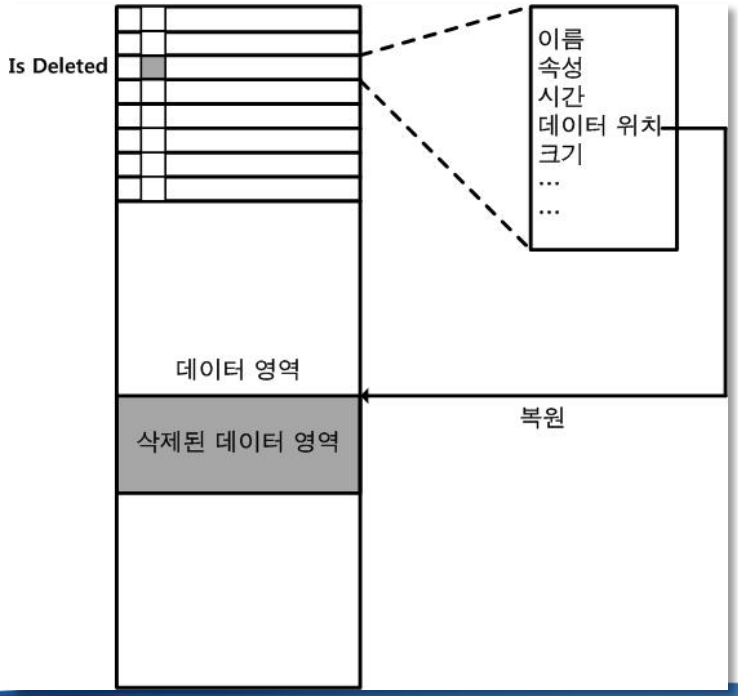
저장매체 복구 기술

- **물리적 복구** : 저장매체의 물리/전자적 복구. 물리적 또는 전자적 단/합선으로 훼손된 저장매체를 정상 상태로 복구하는 기술
- **논리적 복구** : 삭제/훼손된 파일 및 파일 시스템을 복구하는 기술

안티 포렌식 대응 기술 – 데이터 복구

파일시스템 메타데이터기반 복구

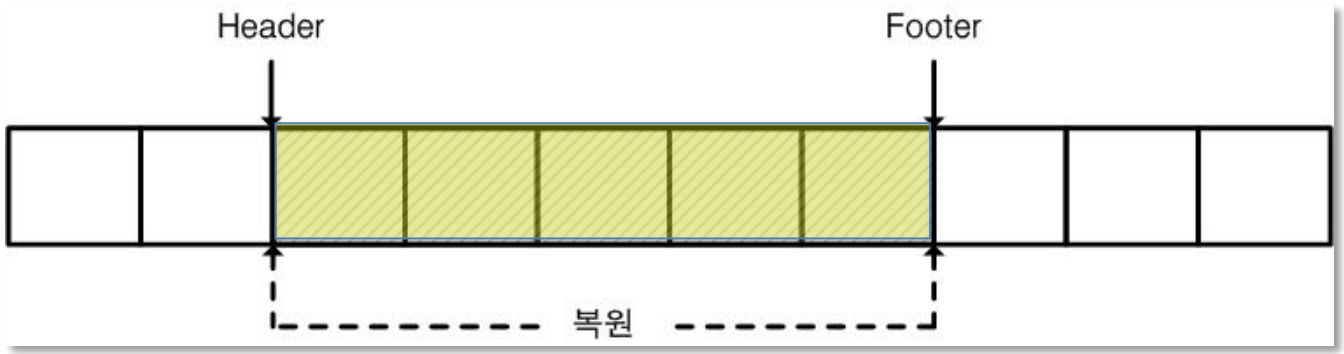
- 파일의 메타 데이터의 **'삭제 플래그'** 를 참조하여 복구
  - 파일 삭제 시 데이터 영역이나 메타데이터 영역을 덮어쓰지 않기 때문에 가능
  - 다른 파일로 덮이지 않았다면 복구 가능



안티 포렌식 대응 기술 – 데이터 복구

파일 시스템 정보를 얻을 수 없는 경우의 복구

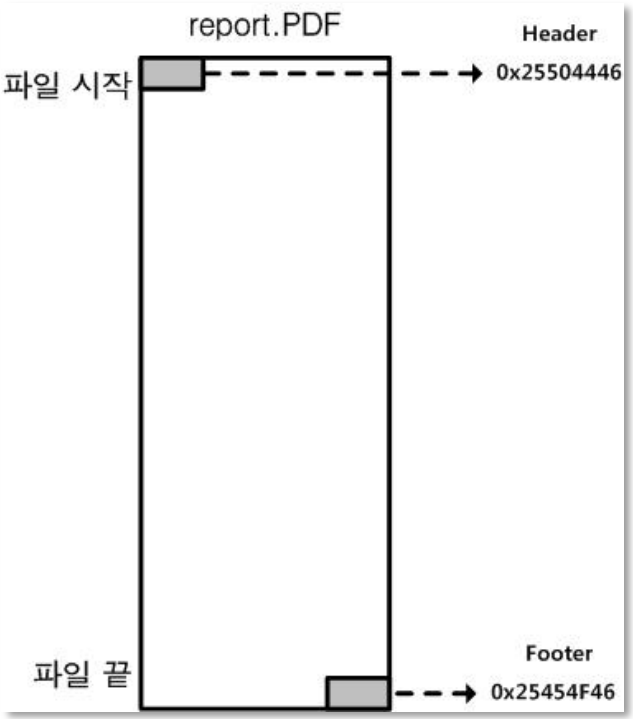
- 파일 시스템에서 얻을 수 있는 정보 없이 **'파일 자체 정보'** 기반 복구
  - 즉, 파일의 고유한 특성이 있는 파일만 복구 가능
- 연속적으로 존재하는 파일에 대한 복구는 대부분 가능, 조각난 경우는 어려움
- 추출된 파일이 올바른 파일이라는 보장이 없음
- 많은 시간이 소요됨

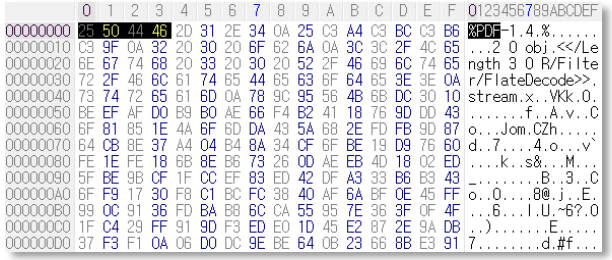


파일 카빙 기법-1

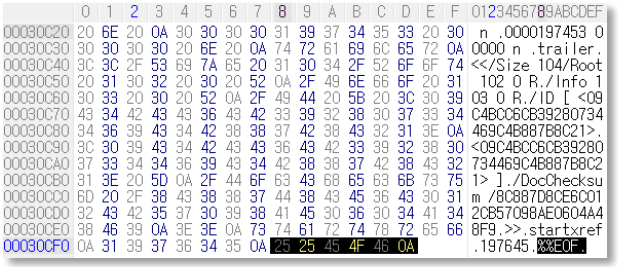
파일의 Header와 Footer 정보

- 일부 파일은 파일의 시작과 끝을 알 수 있는 고유한 Header와 Footer를 가짐
  - PDF, GIF. PNG, JPG, ALZ, ZIP, RAR, MPG …





	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00000000	25	50	44	46	2D	31	2E	34	0A	25	C3	A4	C3	BC	C3	B6	%PDF-1.4.%.....
00000010	C3	9F	0A	32	20	30	20	6F	62	6A	0A	3C	3C	2F	4C	65	...2 0 obj.<<⁄Le
00000020	6E	67	74	68	20	33	20	30	20	52	2F	46	69	6C	74	65	ngth 3 0 R⁄Filte
00000030	72	2F	46	6C	61	74	65	44	65	63	6F	64	65	3E	3E	0A	r⁄FlateDecode>>.
00000040	73	74	72	65	61	6D	0A	78	9C	95	56	4B	6B	DC	30	10	stream.x..VKk.O.
00000050	BE	EF	AF	D0	B9	B0	AE	66	F4	B2	41	18	76	9D	DD	43	.......f..A.v..C
00000060	6F	81	85	1E	4A	6F	6D	DA	43	5A	68	2E	FD	FB	9D	87	o...Jom.CZh.....
00000070	64	CB	8E	37	A4	04	B4	8A	34	CF	6F	BE	19	D9	76	60	d..7....4.o...v`
00000080	FE	1E	FE	18	6B	8E	B6	73	26	0D	AE	EB	4D	18	02	ED	....k..s&...M...
00000090	5F	BE	9B	CF	1F	CC	EF	83	ED	42	DF	A3	33	B6	B3	43	_........B..3..C
000000A0	6F	F9	17	30	F8	C1	BC	FC	38	40	AF	6A	BF	0E	45	FF	o..0....8@.j..E.
000000B0	99	0C	91	36	FD	BA	B8	6C	CA	55	95	7E	36	3F	0F	4F	...6...l.U.~6?.O
000000C0	1F	C4	29	FF	91	9D	F3	ED	E0	1D	45	E2	87	2E	9A	DB	..)........E.....
000000D0	37	F3	F1	0A	06	D0	DC	9E	BE	64	0B	23	66	8B	E3	91	7........d.#f...

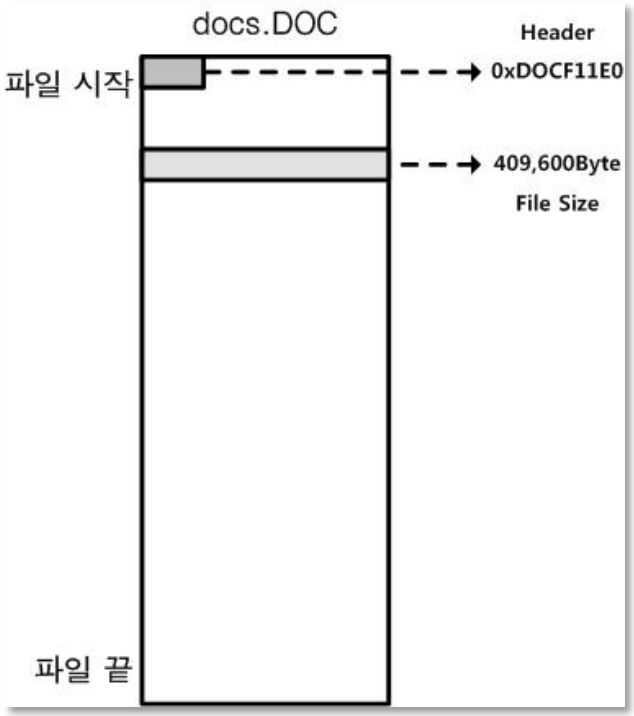


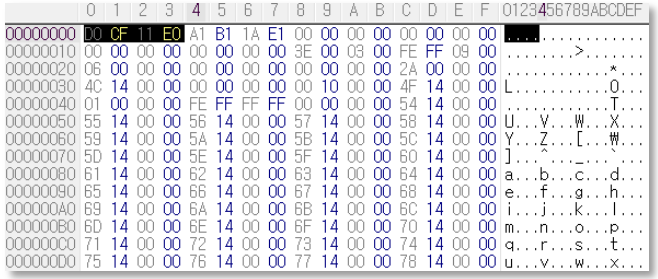
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00030C20	20	6E	20	0A	30	30	30	30	31	39	37	34	35	33	20	30	n .0000197453 0
00030C30	30	30	30	30	20	6E	20	0A	74	72	61	69	6C	65	72	0A	0000 n .trailer.
00030C40	3C	3C	2F	53	69	7A	65	20	31	30	34	2F	52	6F	6F	74	<<⁄Size 104⁄Root
00030C50	20	31	30	32	20	30	20	52	0A	2F	49	6E	66	6F	20	31	102 0 R⁄Info 1
00030C60	30	33	20	30	20	52	0A	2F	49	44	20	5B	20	3C	30	39	03 0 R⁄ID [<09
00030C70	43	34	42	43	43	36	43	42	33	39	32	38	30	37	33	34	C4BCC6CB39280734
00030C80	34	36	39	43	34	42	38	38	37	42	38	43	32	31	3E	0A	469C4B887B8C21>.
00030C90	3C	30	39	43	34	42	43	43	36	43	42	33	39	32	38	30	<09C4BCC6CB39280
00030CA0	37	33	34	34	36	39	43	34	42	38	38	37	42	38	43	32	734469C4B887B8C2
00030CB0	31	3E	20	5D	0A	2F	44	6F	63	43	68	65	63	6B	73	75	1>]⁄DocChecksu
00030CC0	6D	20	2F	38	43	38	38	37	44	38	43	45	36	43	30	31	m ⁄8C887D8CE6C01
00030CD0	32	43	42	35	37	30	39	38	41	45	30	36	30	34	41	34	2CB57098AE0604A4
00030CE0	38	46	39	0A	3E	3E	0A	73	74	61	72	74	78	72	65	66	8F9.>>.startxref
00030CF0	0A	31	39	37	36	34	35	0A	25	25	45	4F	46	0A			.197645.%%EOF.

파일 카빙 기법-2

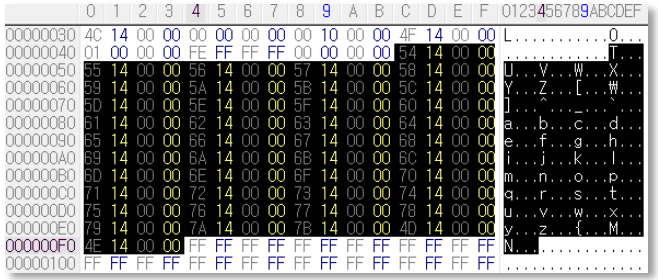
파일의 Header와 File size 정보

- 일부 파일은 파일의 시작과 크기를 알 수 있는 정보를 포함하고 있음
  - DOC, ODT, ODS, BMP, AVI, ASF, WAV …





	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00000000	D0	CF	11	E0	A1	B1	1A	E1	00	00	00	00	00	00	00	00	....á±.á.....
00000010	00	00	00	00	00	00	00	00	3E	00	03	00	FE	FF	09	00	........>.....
00000020	06	00	00	00	00	00	00	00	00	00	00	00	2A	00	00	00	..........*...
00000030	4C	14	00	00	00	00	00	00	00	10	00	00	4F	14	00	00	L.........O...
00000040	01	00	00	00	FE	FF	FF	FF	00	00	00	00	54	14	00	00	............T...
00000050	55	14	00	00	56	14	00	00	57	14	00	00	58	14	00	00	U...V...W...X...
00000060	59	14	00	00	5A	14	00	00	5B	14	00	00	5C	14	00	00	Y...Z...[...₩...
00000070	5D	14	00	00	5E	14	00	00	5F	14	00	00	60	14	00	00	]...^..._...`...
00000080	61	14	00	00	62	14	00	00	63	14	00	00	64	14	00	00	a...b...c...d...
00000090	65	14	00	00	66	14	00	00	67	14	00	00	68	14	00	00	e...f...g...h...
000000A0	69	14	00	00	6A	14	00	00	6B	14	00	00	6C	14	00	00	i...j...k...l...
000000B0	6D	14	00	00	6E	14	00	00	6F	14	00	00	70	14	00	00	m...n...o...p...
000000C0	71	14	00	00	72	14	00	00	73	14	00	00	74	14	00	00	q...r...s...t...
000000D0	75	14	00	00	76	14	00	00	77	14	00	00	78	14	00	00	u...v...w...x...



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00000030	4C	14	00	00	00	00	00	00	00	10	00	00	4F	14	00	00	L.........O...
00000040	01	00	00	00	FE	FF	FF	FF	00	00	00	00	54	14	00	00	............T...
00000050	55	14	00	00	56	14	00	00	57	14	00	00	58	14	00	00	U...V...W...X...
00000060	59	14	00	00	5A	14	00	00	5B	14	00	00	5C	14	00	00	Y...Z...[...₩...
00000070	5D	14	00	00	5E	14	00	00	5F	14	00	00	60	14	00	00	]...^..._...`...
00000080	61	14	00	00	62	14	00	00	63	14	00	00	64	14	00	00	a...b...c...d...
00000090	65	14	00	00	66	14	00	00	67	14	00	00	68	14	00	00	e...f...g...h...
000000A0	69	14	00	00	6A	14	00	00	6B	14	00	00	6C	14	00	00	i...j...k...l...
000000B0	6D	14	00	00	6E	14	00	00	6F	14	00	00	70	14	00	00	m...n...o...p...
000000C0	71	14	00	00	72	14	00	00	73	14	00	00	74	14	00	00	q...r...s...t...
000000D0	75	14	00	00	76	14	00	00	77	14	00	00	78	14	00	00	u...v...w...x...
000000E0	79	14	00	00	7A	14	00	00	7B	14	00	00	4D	14	00	00	y...z...{...M...
000000F0	4E	14	00	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	N..............
00000100	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	....

파일 카빙 기법-3

파일이 연속적이지 않고 조각난 경우

- 조각난 파일이 생성되는 이유
  - 파일을 저장할 충분한 연속 공간이 없을 경우
  - 기존 파일에 데이터가 추가될 때, 파일의 후반부 영역에 할당되지 않은 영역의 크기가 충분하지 않은 경우
- 파일 포맷의 특성을 이용한 여러 복구 방안이 연구 중
- Pattern Recognition, 통계 분석 등

안티 포렌식 대응 기술 – 데이터 암호화

- 데이터 암호화
  - Zip, Rar 등과 같은 압축파일에 암호화 기법을 적용하여, 증거확보를 어렵게 함
  - MS 오피스 및 한글 파일 등과 같은 문서를 암호화하여, 정보를 은폐하는데 활용되고 있음

안티 포렌식 대응 기술 – 데이터 암호화

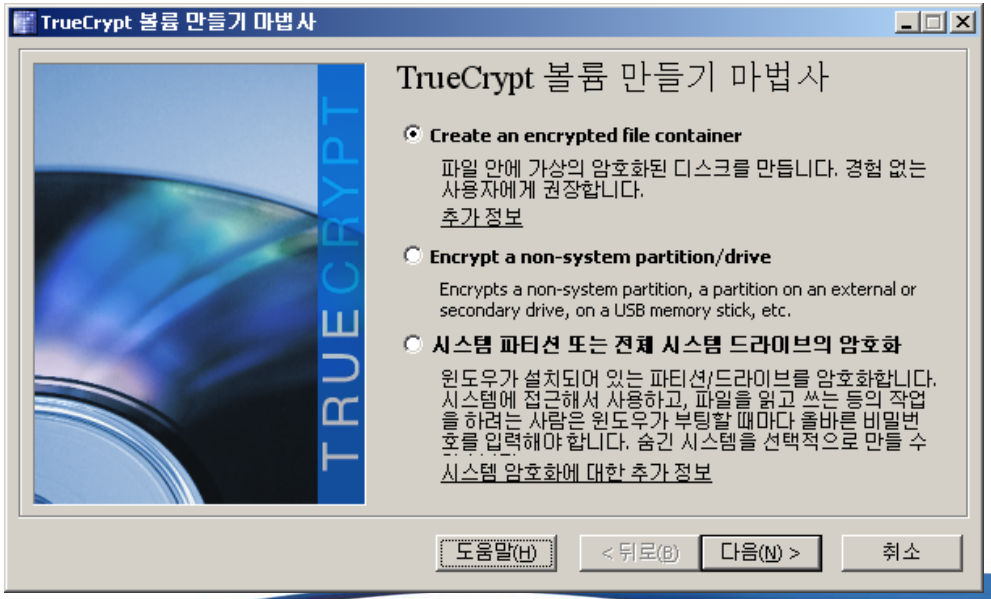
- **TrueCrypt - http://www.truecrypt.org**
  - 오픈 소스 디스크 암호화 도구
    - Windows XP/2003/Vista/2008, Mac OS and Linux
  - 지원 알고리즘

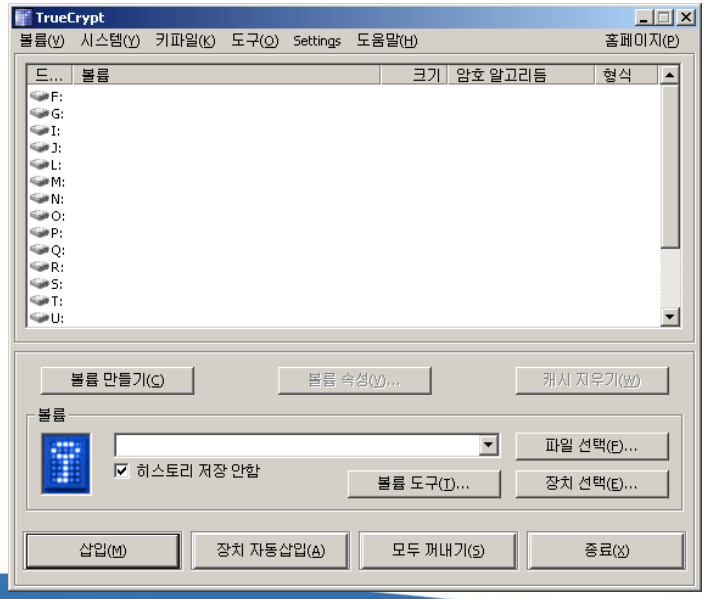
Algorithm	Key Size(Bits)	Block Size(Bits)
AES	256	128
Serpent	256	128
Twofish	256	128
AES-Twofish	256; 256	128
AES-Twofish-Serpent	256; 256; 256	128
Serpent-AES	256; 256	128
Serpent-Twofish-AES	256; 256; 256	128
Twofish-Serpent	256; 256	128

  - Current Version
    - TrueCrypt 6.1

안티 포렌식 대응 기술 – 데이터 암호화

- **TrueCrypt** 기능
  - 가상 디스크 암호화 : 파일 형태의 암호화 데이터를 볼륨으로 가상 마운트
  - 스토리지 암호화 : USB, Hard Disk 볼륨을 암호화
  - OS가 설치된 파티션 암호화
    - 복호화 기능을 가진 CD로 부팅하여 인증 (pre-boot authentication)



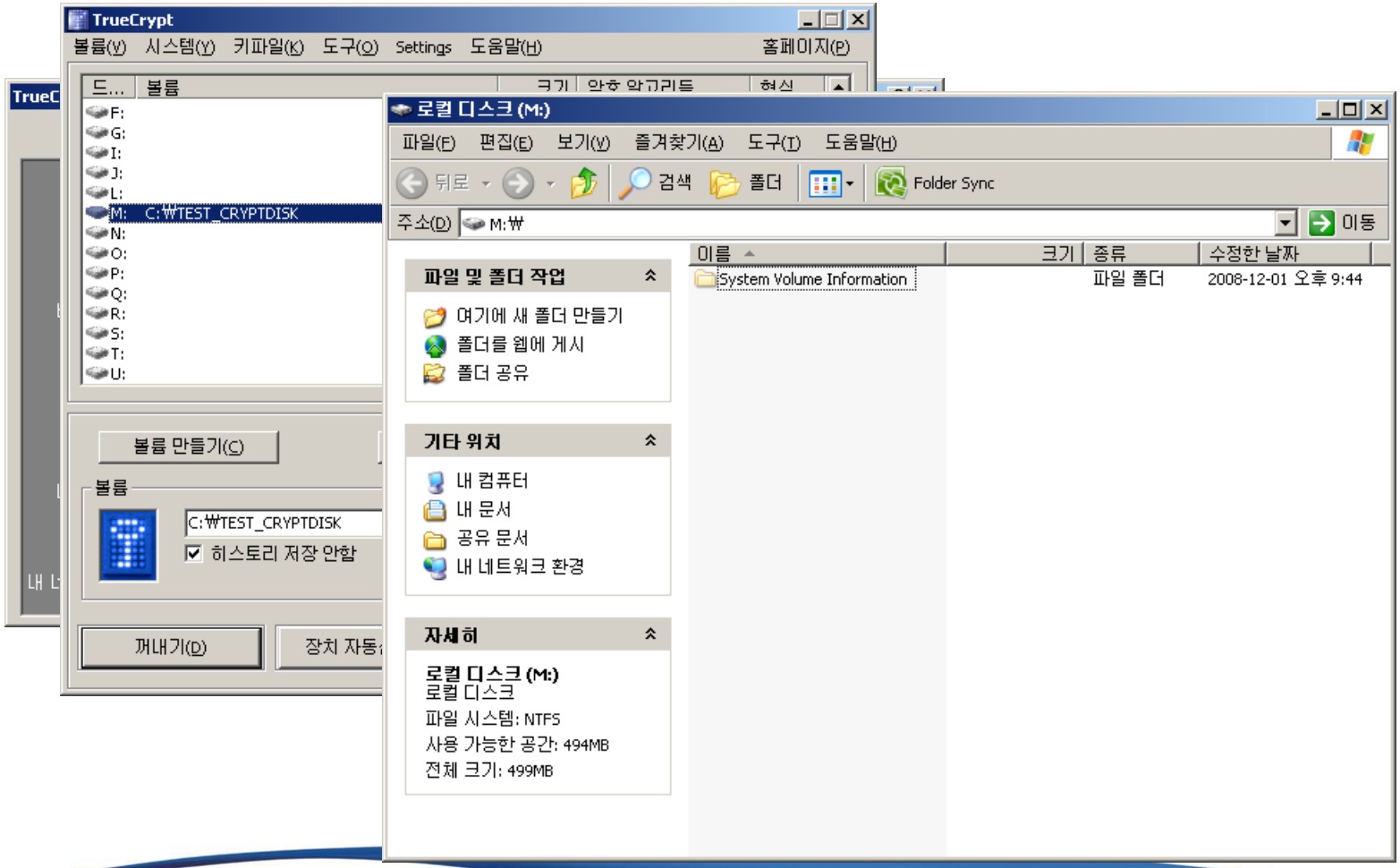


안티 포렌식 대응 기술 – 데이터 암호화

✓ TrueCrypt 암호화 볼륨 생성

안티 포렌식 대응 기술 – 데이터 암호화

✓ TrueCrypt 암호화 볼륨 마운트



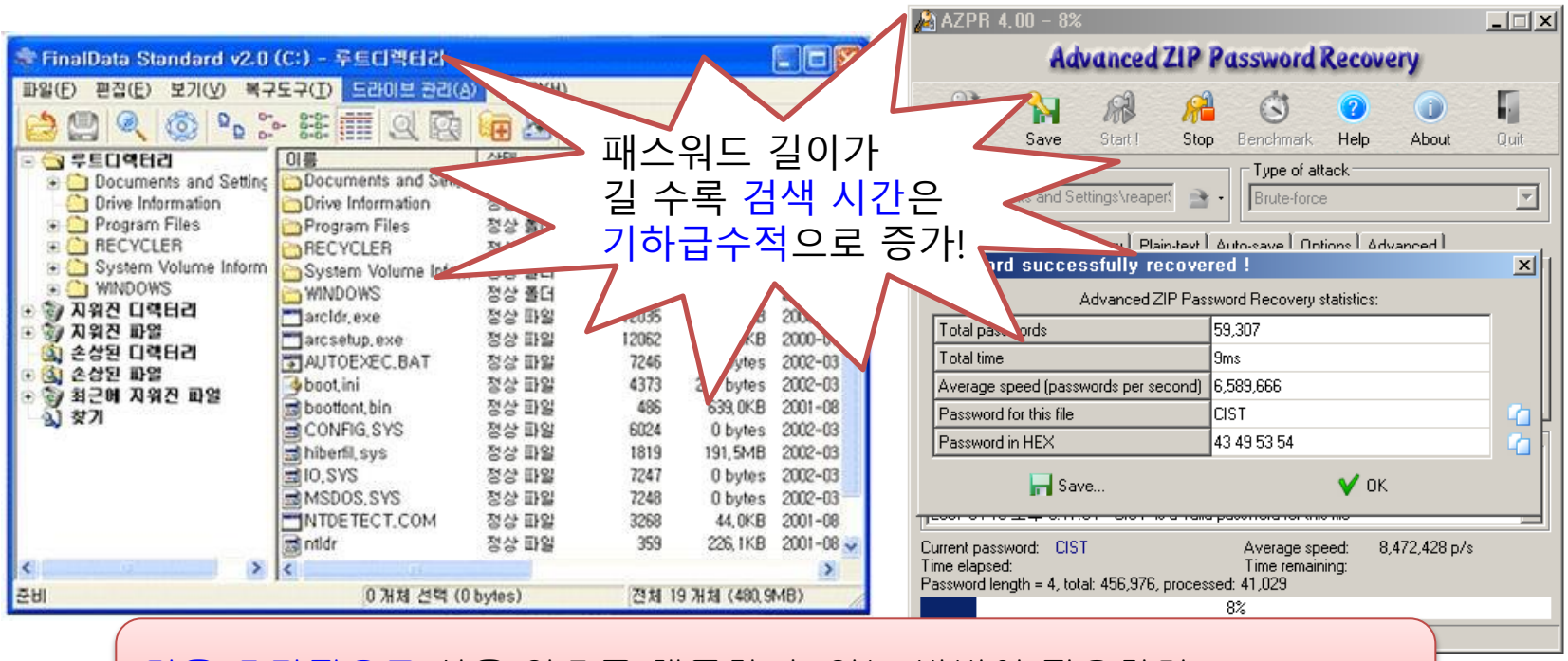
안티 포렌식 대응 기술 – 패스워드 검색

- **암호화된 데이터는 대부분 사용자가 입력한 패스워드를 키로 사용**

- **패스워드 검색 방법**
  - 사회공학적 기법
  - 사전 공격
  - 전수 조사

안티 포렌식 대응 기술 – 패스워드 검색

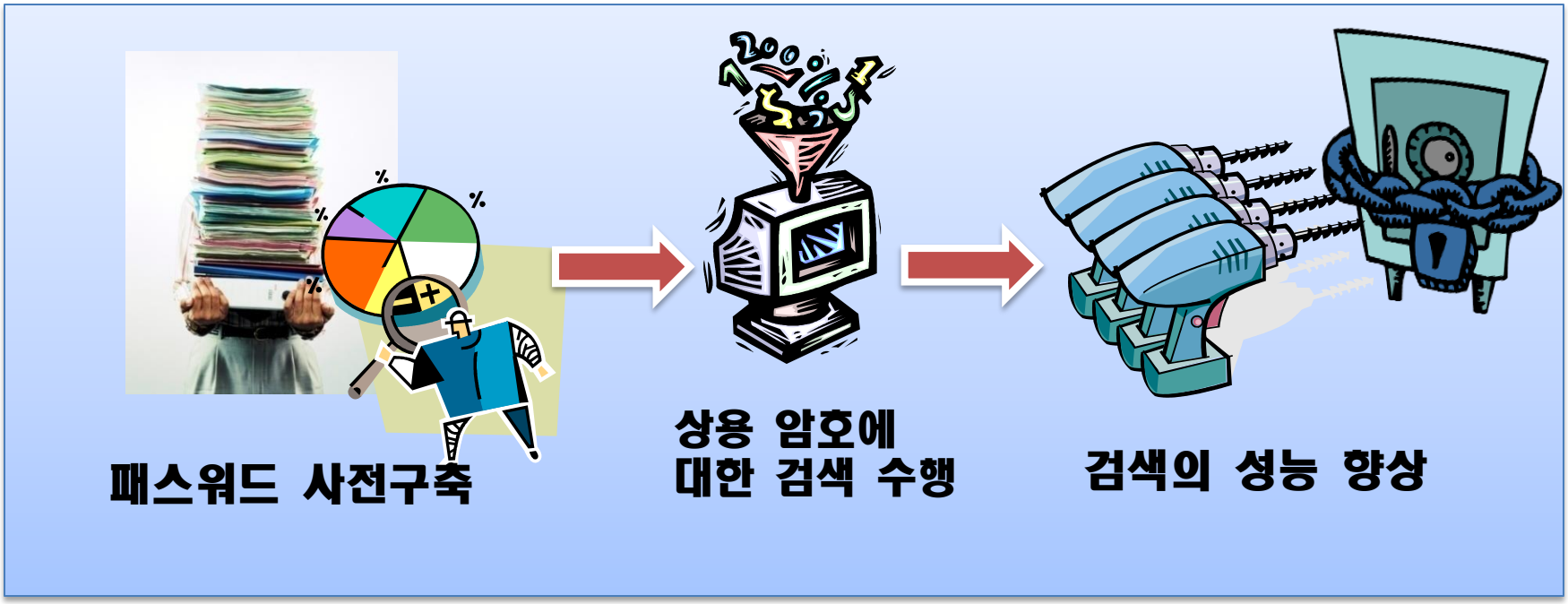
- 전수조사 기법의 적용
  - 모든 문자열을 대상으로 선정하여, 검색을 수행하는 기법
  - 암호화된 데이터 파일의 패스워드를 전수조사
  - Elcomsoft 社의 'Password Recovery Tool'이 대표적



더욱 효과적으로 상용 암호를 해독할 수 있는 방법이 필요하며,
사전구성을 통한 암호 해독이 대안으로써 활용이 가능

안티 포렌식 대응 기술 – 패스워드 검색

- 사전 공격 기법의 적용
  - 체계적인 사전 구축을 통하여 패스워드 검색 속도 향상 가능
  - 빠른 시간 내에 패스워드 검색이 가능하며, 전수조사 기법보다 효율적임



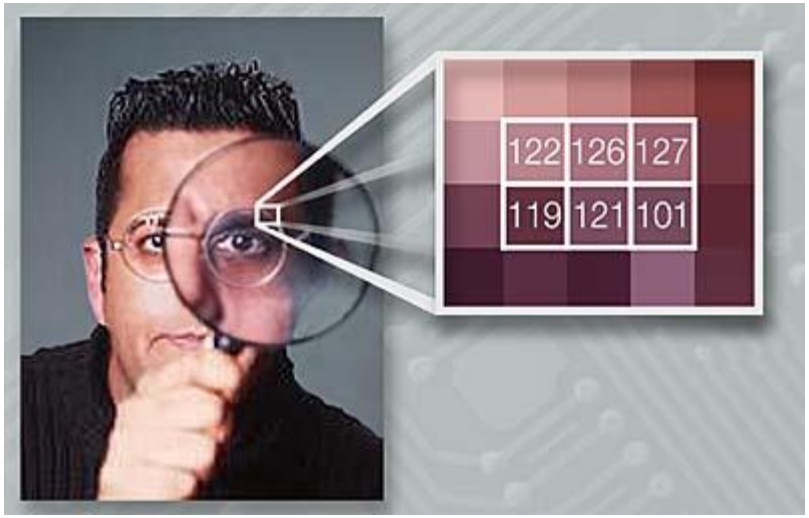
안티 포렌식 대응 기술 – 심층 암호 분석

- **멀티미디어 파일 분석**
  - 이미지, 동영상 등의 파일에 은닉된 데이터 탐지하는 기술
  - 영상 분석, 색상 분석, 통계 분석 등 사용

- **문서 파일 분석**
  - MS Office, 한글 등의 파일에 은닉된 데이터 탐지 기술
  - 저장 형식 분석을 통해 탐지

안티 포렌식 대응 – 스테가노그라피

- **Steganography**
  - 메시지가 전송되고 있다는 사실 즉, 통신의 존재를 숨기는 기술로서 이미지 및 오디오 파일과 같은 다양한 디지털 매체를 통해 메시지를 은닉하여 전송하는 기술
    - 모르는 사람이 보면 평범한 사진에 불과하지만 약속된 수신자는 그 안에 메시지를 확인할 수 있는 기술

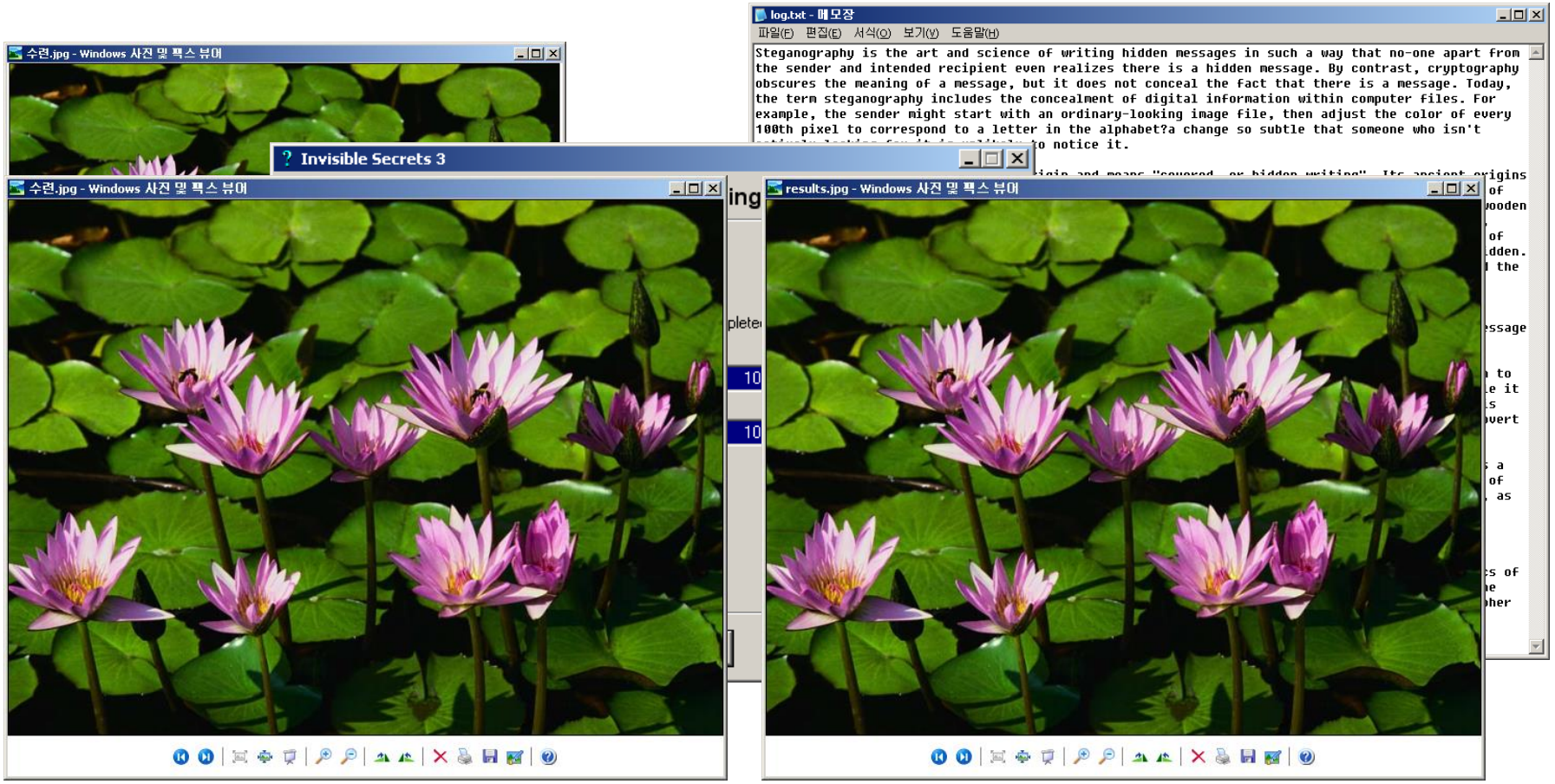


안티 포렌식 대응 – 스테가노그라피

- **Invisible Secrets 3 – http://www.invisiblesecrets.com**
  - 지원 데이터
    - BMP, JPEG, HTML, PNG, WAV
  - Windows 95/98, NT, XP 지원
  - 알고리즘
    - AES(Rijndael), RC4, Twofish, Cast128, Ghost, Diamond 2, Sapphire, Blowfish

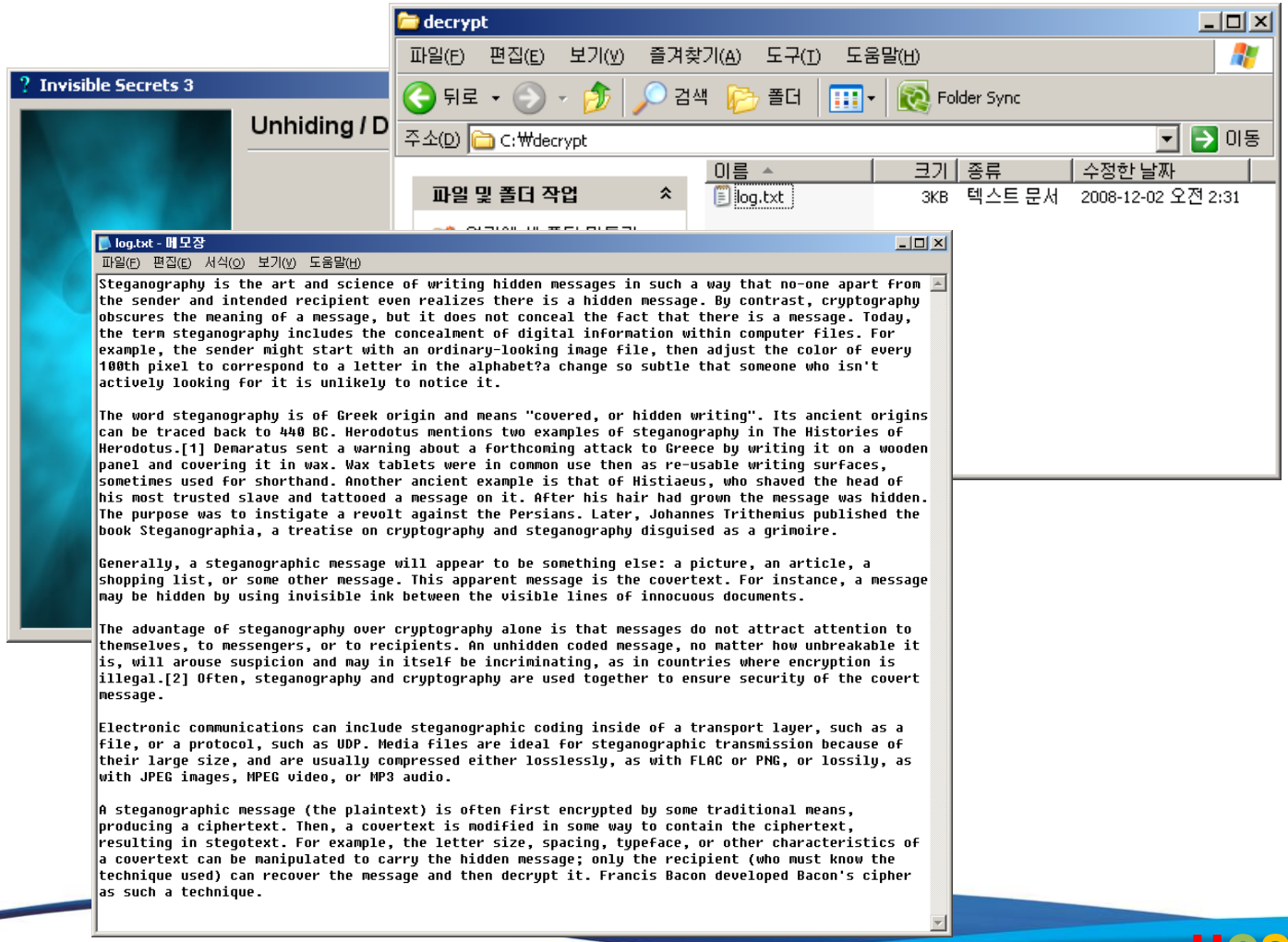
안티 포렌식 대응 – 스테가노그라피

- **Invisible Secrets 3** 데이터 은닉



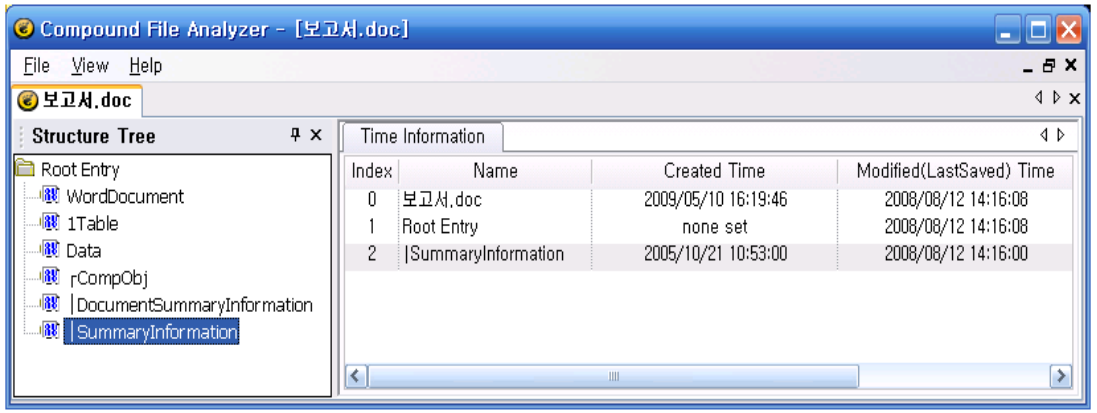
안티 포렌식 대응 – 스테가노그라피

- **Invisible Secrets 3** 은닉 데이터 추출



안티 포렌식 대응 기술 – 파일 내부의 시간 정보 분석

- 파일 시스템 상에 저장되는 시간 정보는 변조가 용이
- 응용 프로그램에 의해 파일 내부에 저장되는 시간 정보는 해당 파일의 저장 형식을 알지 못하면 변경하기 매우 어려움



문서 파일 내부 시간 정보 분석 도구 : CFA

안티 포렌식 대응 기술 – 기타 분석 기술

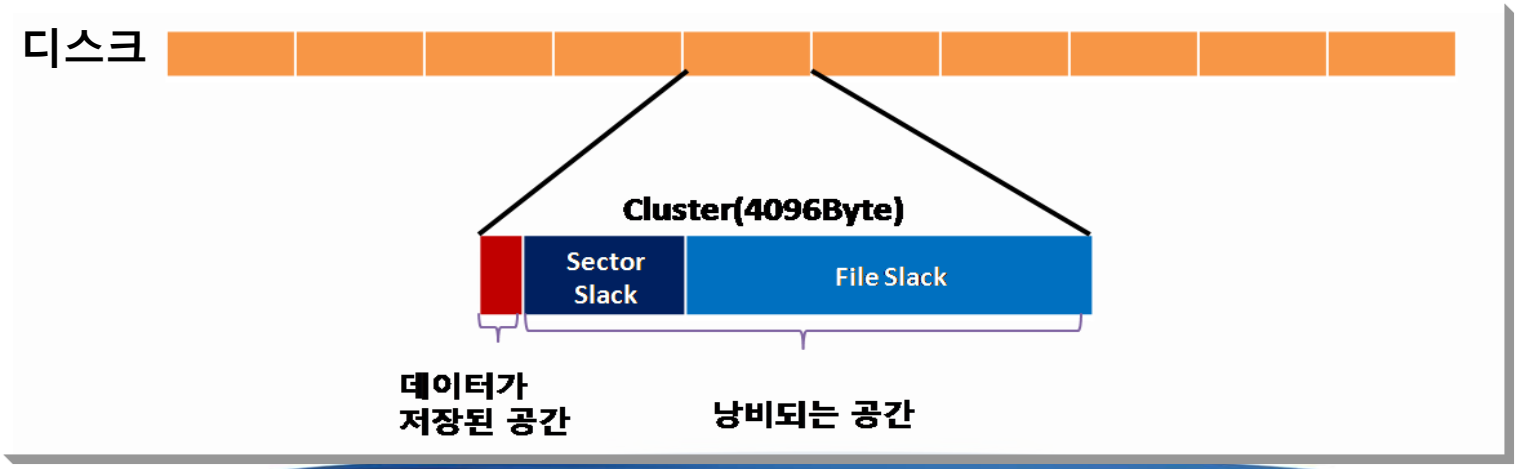
- **일관성 분석**
  - 시간의 연속성 특성을 이용
  - 파일, 파일의 메타데이터, 로그 등 이용

- **연관 관계 분석**
  - 서로 다른 이벤트 사이의 연관 관계를 밝히는 분석 방법
  - 통계, 마이닝 기법 등 사용하여 둘 이상의 서로 다른 이벤트 사이의 관계를 밝히는 것

파일시스템 – 슬랙 공간

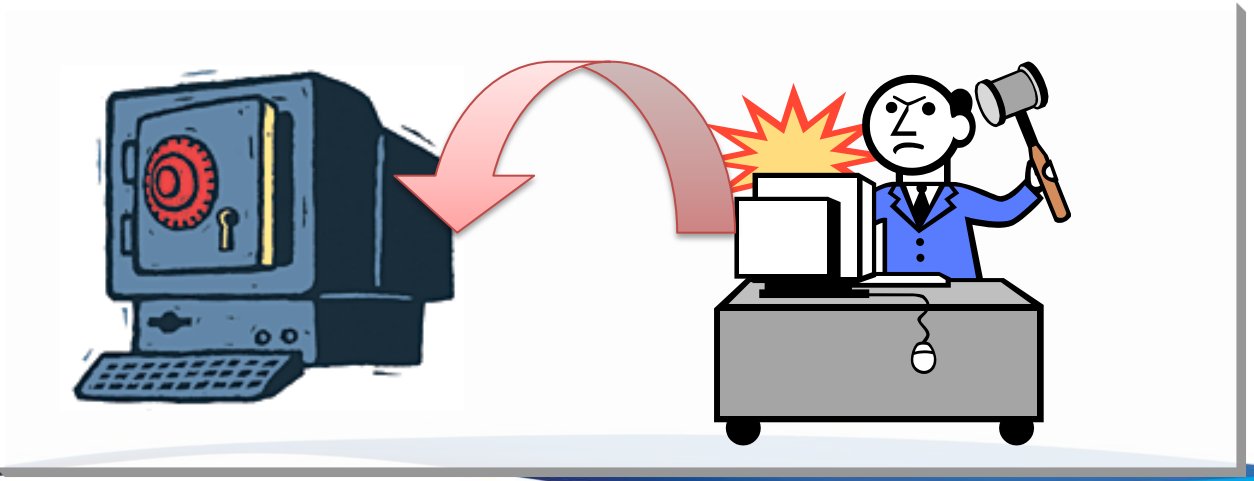
- 파일시스템
  - 디스크 드라이브에 파일을 저장하고 탐색이 용이하도록 설계된 관리 시스템
    - FAT(FAT12, FAT16, FAT32, exFAT), NTFS, HFS/HFS+, HPFS
    - Ext2, Ext3, ISO 9660, ZFS, VxFS, Journaling file system, versioning file system

- 슬랙 공간이란?
  - Slack Space : 디스크에서 뜻하지 않게 낭비되는 공간
  - Sector(RAM) Slack : 섹터단위(512 bytes)로 접근하는 디스크의 특성에 따른 낭비
  - File Slack : Cluster, Block 단위로 저장되는 특성에 따른 낭비



안티 포렌식 기술 대응방안

- **Anti-Forensic**에 대한 대응
  - 프라이버시 및 개인 정보 보호라는 긍정적인 측면도 있지만, 범죄자가 범행직후 증거를 없애는 용도로 사용하는 경우에는 컴퓨터 범죄 수사에 많은 어려움을 초래할 수 있음
  - Anti-Forensic 기술은 앞으로도 계속 발전되고 대중화 될 것이 예상되며, 이에 대응할 수 있는 기술과 정책적 기반이 필요함



Q & A