디지털 증거 분석 기술

김종성
국민대학교

Email: jskim@kookmin.ac.kr

목 차

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

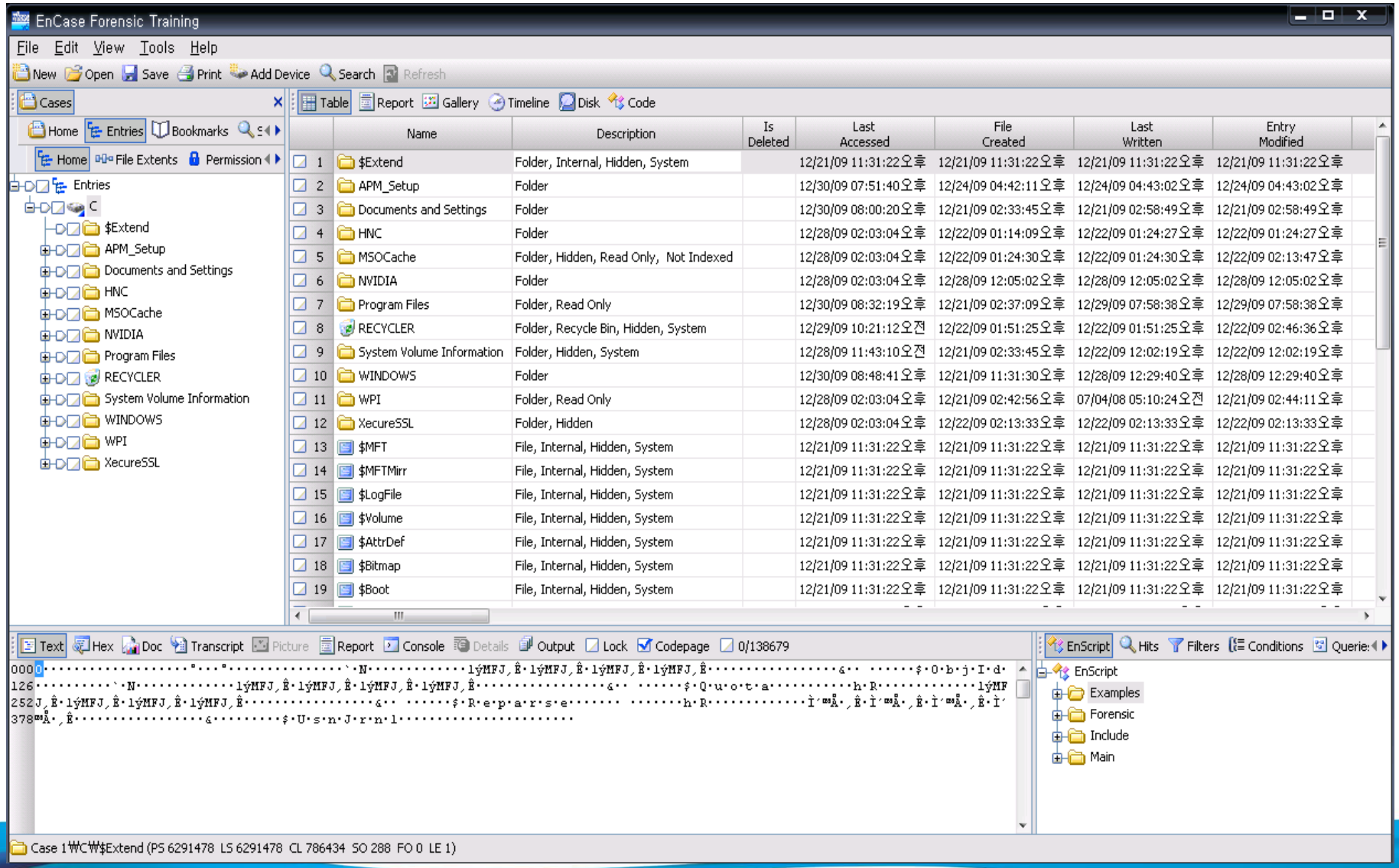
디스크 브라우징 기술

- **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

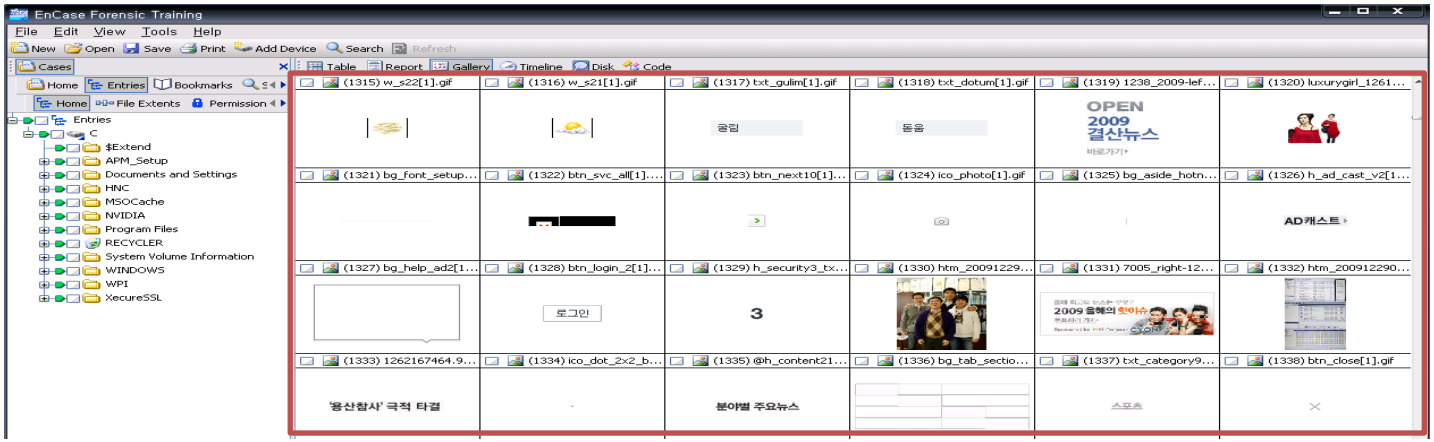
- **EnCase의 디스크 브라우징 기능**



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

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

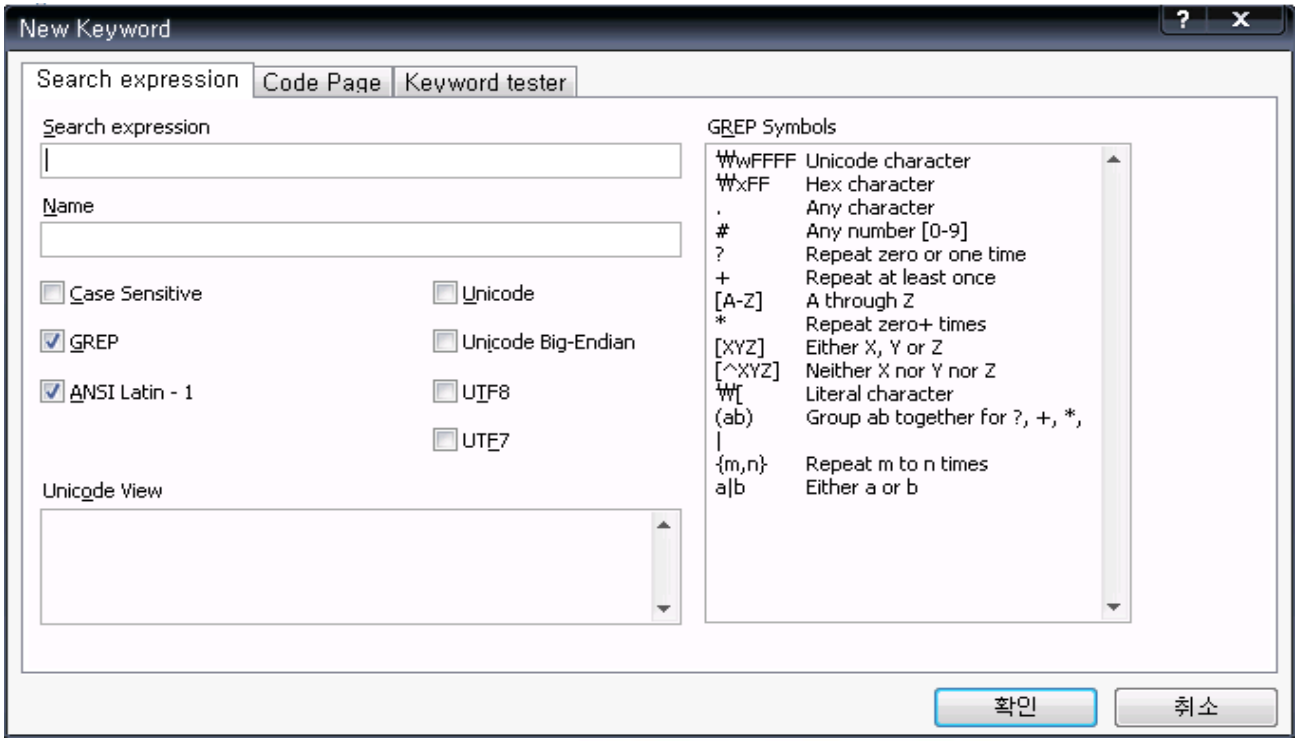
- **포렌식 조사/분석은 연속되는 검색의 반복**
  - 모든 파일들의 키워드, Signature에 대해 검색을 반복해야 함
  - 잘 알려진 파일은 검색 대상에서 제외하고, 주목해서 검색할 대상을 선정하여, 검색 범위를 축소하는 것이 중요함.
  - 발전된 형태의 검색기술을 사용하여 조사/분석 단계에 투입되는 시간 비용을 줄일 수 있어야 함

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-Hashed Search (2)

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

```
"SHA-1",                                    "MD5",                                  "CRC32",   "FileName",       "FileSize","ProductCode"
"00000F6ED90D946C057B55545597C3125lDC24E4","F4129AC77F806601BDD44620C17675E7","38CC50B7","004i200r.gif"   ,  1551,228,     "WIN"
"00000FF9D0ED9A6B53BC6A9364C07074DE1565F3","A5D49D6DA9D78FD1E7C32D58BC7A46FB","2D729A1E","cmnres.pdb.dll",76800,2471,     "WIN"
"00000FF9D0ED9A6B53BC6A9364C07074DE1565F3","A5D49D6DA9D78FD1E7C32D58BC7A46FB","2D729A1E","cmnres.pdb.dll",76800,2704,     "WIN"
"00000FF9D0ED9A6B53BC6A9364C07074DE1565F3","A5D49D6DA9D78FD1E7C32D58BC7A46FB","2D729A1E","cmnres.pdb.dll",76800,2741,     "WIN"
"00000FF9D0ED9A6B53BC6A9364C07074DE1565F3","A5D49D6DA9D78FD1E7C32D58BC7A46FB","2D729A1E","cmnres.pdb.dll",76800,2797,     "WIN"
"00000FF9D0ED9A6B53BC6A9364C07074DE1565F3","A5D49D6DA9D78FD1E7C32D58BC7A46FB","2D729A1E","cmnres.pdb.dll",76800,2912,     "WIN"
```

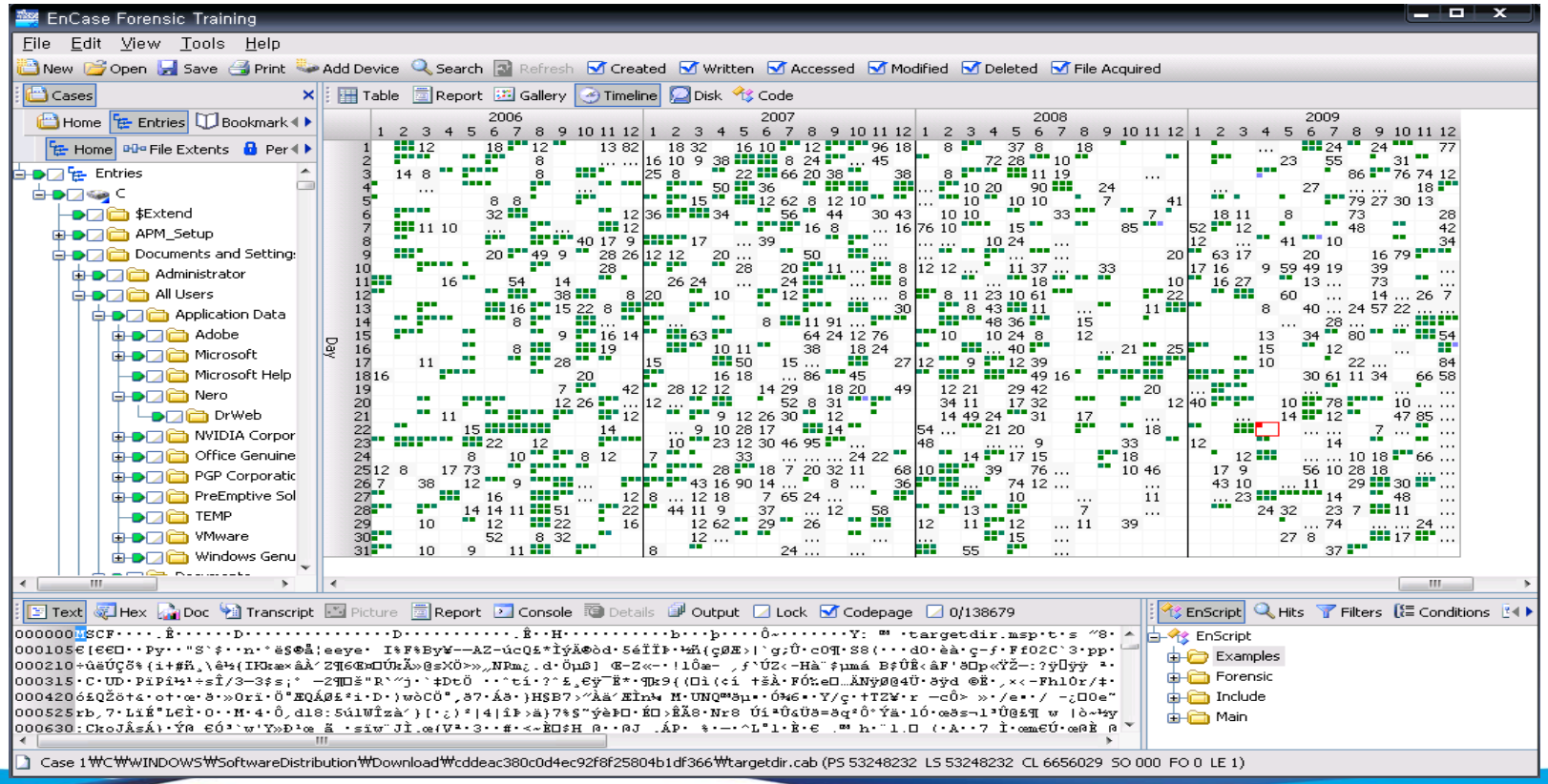
검색 기술-Hashed Search (3)

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

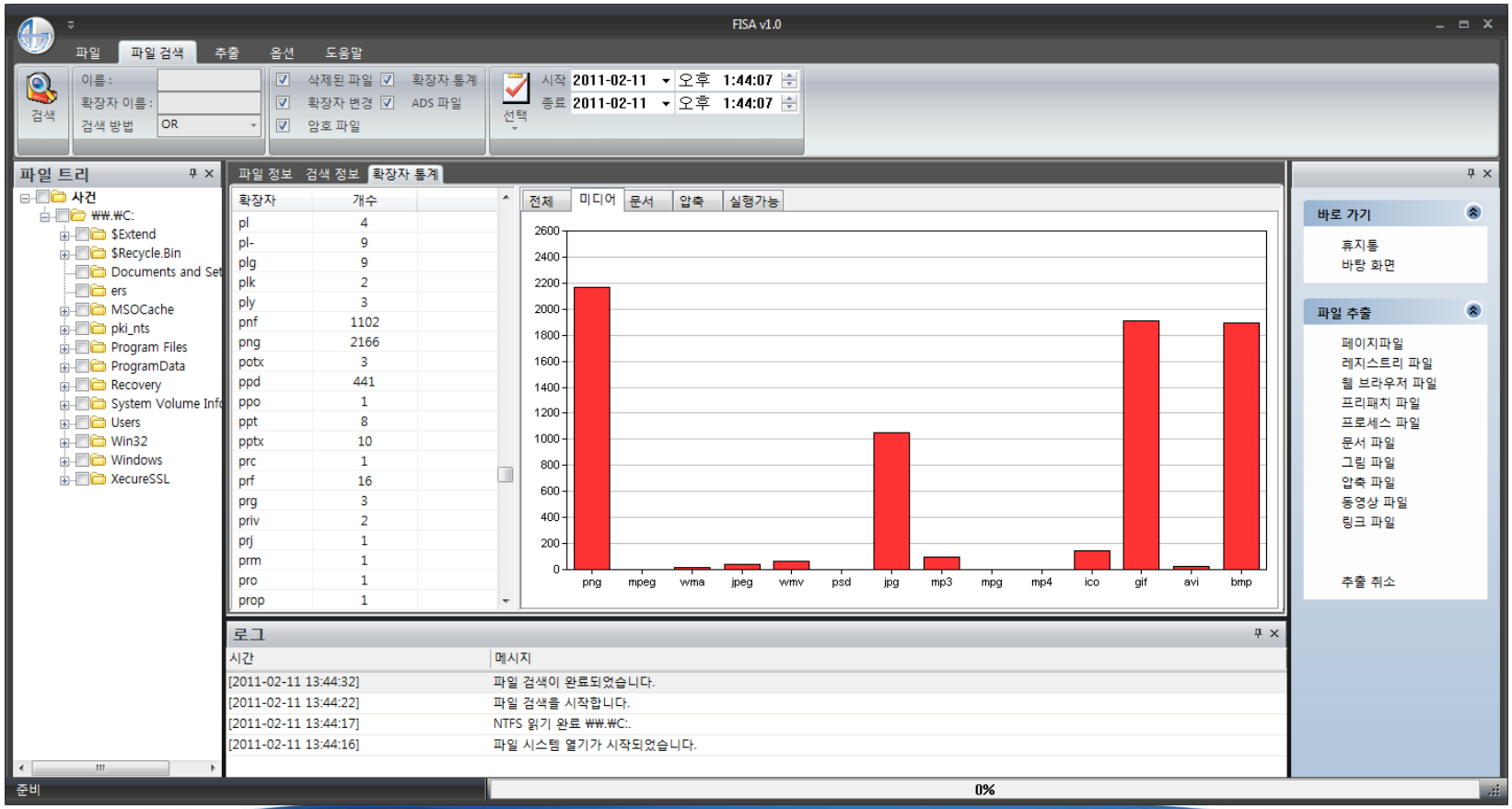
타임라인 분석

- **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



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

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

안티 포렌식 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

데이터 영구 삭제

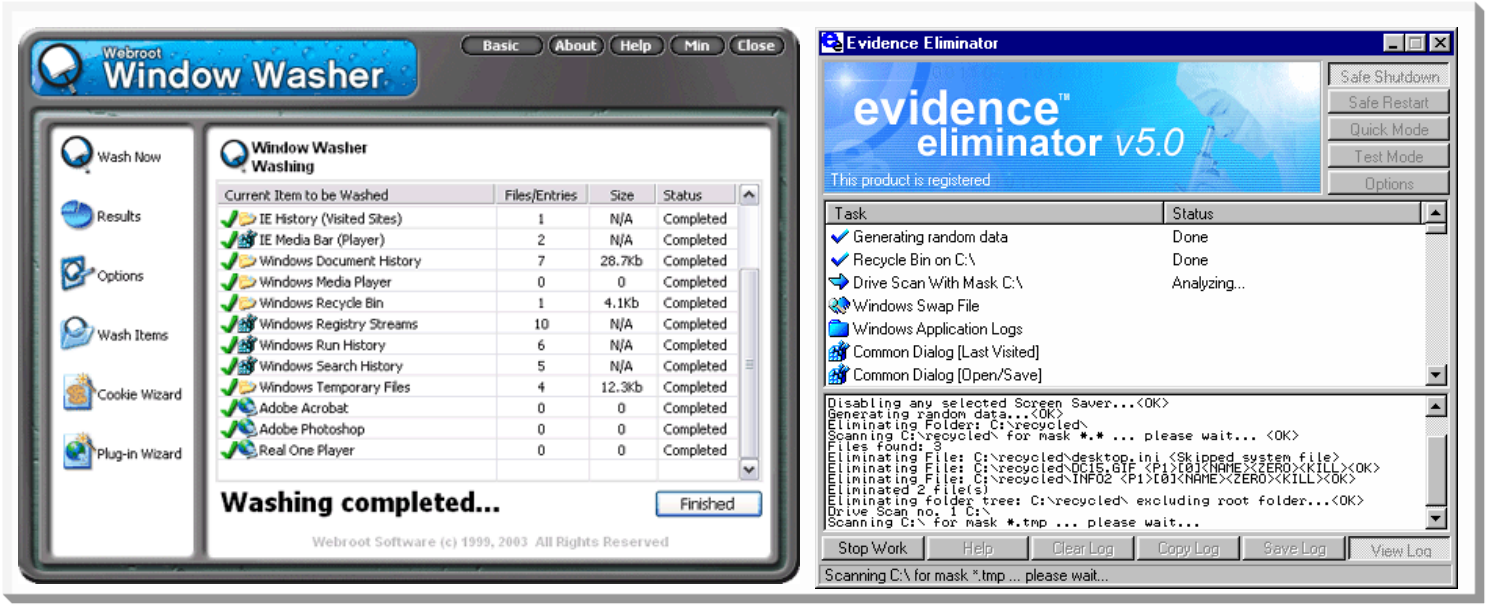
- **Disk Wipe**
  - 하드디스크의 기존 데이터를 완벽히 제거하고 모든 Sector의 내용을 0으로 만드는 과정
- **디가우저 (소자, Degausser)**
  - 하드디스크나 테이프에 강력한 자기장을 노출시켜 기록된 데이터를 파괴하고 복구가 불가능하도록 하는 장비

[Disk Wipe S/W]


소자용 전문 제품
(Degausser – BTE)

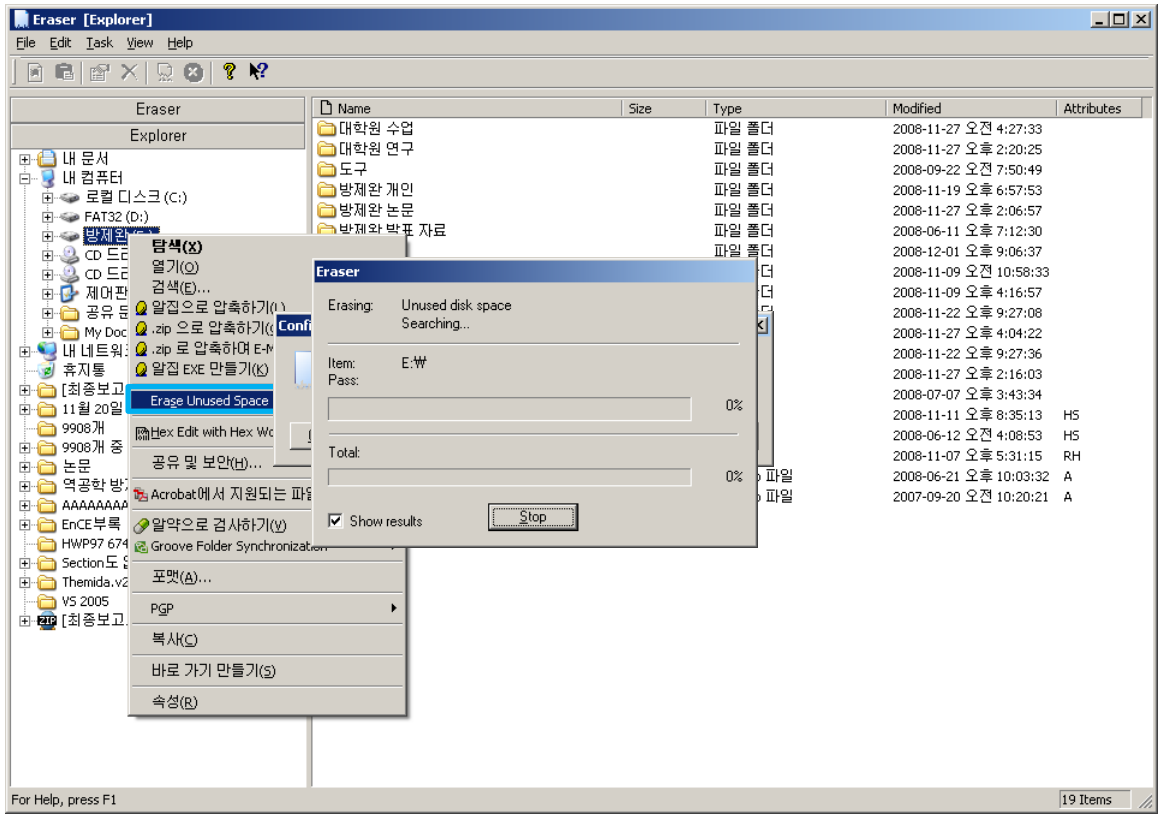
데이터 영구 삭제

- **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



데이터 영구 삭제

- **Eraser 디스크 미사용 영역 완전 삭제**



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

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

데이터 은닉 -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

데이터 은닉 -스테가노그라피

- **Invisible Secrets 3 – http://www.invisiblesecrets.com**
  - 지원 데이터
    - BMP, JPEG, HTML, PNG, WAV
  - Windows 95/98, NT, XP 지원

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

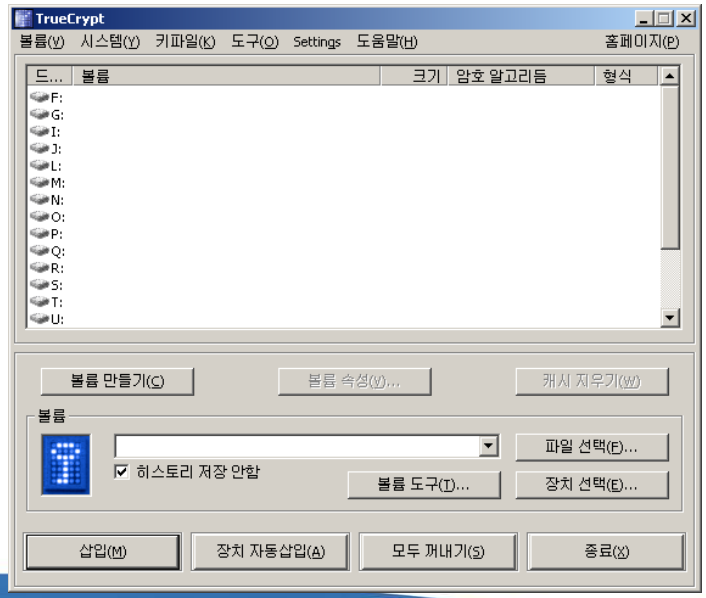
데이터 암호화

- **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

데이터 암호화

- **TrueCrypt 기능**
  - 스토리지 암호화 : USB, Hard Disk 볼륨을 암호화
  - OS가 설치된 파티션 암호화



데이터 암호화

- **모바일 포렌식과 암호화**
  - **카카오톡과 같은 메신저 애플리케이션의 데이터베이스 암호화 지원**
    - 데이터베이스를 획득해도 대화내용 바로 확인 불가
    - 이외 여러 애플리케이션에서도 데이터베이스 암호화 기능이 적용되어 있음

암호화 전 데이터베이스 파일

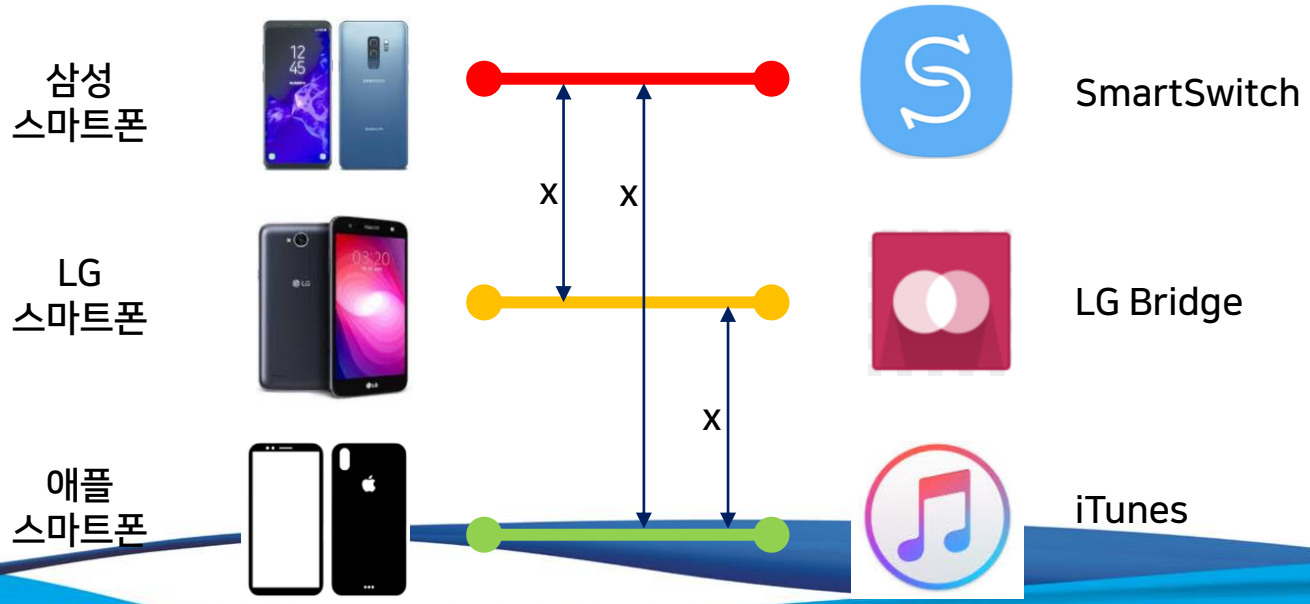
0000h:	53	51	4C	69	74	65	20	66	6F	72	6D	61	74	20	33	00	SQLite format 3.
0010h:	10	00	01	01	00	40	20	20	00	00	00	65	00	00	00	04	.....@ ...e....
0020h:	00	00	00	00	00	00	00	00	00	00	00	02	00	00	00	04	....
0030h:	00	00	00	00	00	00	00	04	00	00	00	01	00	00	00	01	....
0040h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0050h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	65	...............e
0060h:	00	2D	E9	EA	0D	00	00	00	02	0F	45	00	0F	A7	0F	45	.-éê......E..§.E
0070h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....

암호화 후 데이터베이스 파일

0000h:	43	F0	15	AD	4D	F2	1D	91	1F	34	DC	FF	5F	2A	9F	E7	Cð.-Mò.'.4Üÿ_*Ÿç
0010h:	1E	41	4F	DD	B0	86	1D	8F	CA	56	E0	A4	72	68	C5	85	.AOÝ°†..ÊVà¤rhÅ…
0020h:	0E	4D	9E	F1	EB	3D	89	24	27	15	CD	D2	8B	80	F7	42	.Mžñë=‰$'.ÍÒ‹€÷B
0030h:	9C	01	01	DD	55	95	26	0D	71	25	41	21	3A	9A	B6	E4	œ..ÝU•&.q%A!:š¶ä
0040h:	6B	99	C5	F1	18	56	35	D1	E9	F5	F5	17	FE	1D	84	0B	k™Åñ.V5Ñéõõ.þ.„.
0050h:	08	FE	7F	17	6D	4E	2B	8A	B6	4D	FC	A8	BF	4F	CB	FE	.þ..mN+Š¶Mü¨¿OËþ
0060h:	D4	C9	FC	5C	D1	EB	02	11	BA	BD	4B	B9	C6	19	8A	0C	ÔÉü\Ñë..º½K¹Æ.Š.
0070h:	D0	26	B4	8B	C3	A4	A9	D6	E8	8F	B1	F2	87	72	31	0B	Ð&´‹Ã¤©Öè.±ò‡r1.

데이터 암호화

- **모바일 포렌식과 백업**
  - **포렌식 관점에서 스마트폰 백업 데이터 수집의 중요성**
    - 불의의 사고로 스마트폰의 데이터가 손실될 경우, 유일한 복구 방안
    - 백업 데이터에는 대부분의 사용자의 데이터가 포함되므로 포렌식 수사에 큰 도움
    - 다만, 주요 백업 파일은 대부분 평문 형태로 저장되지 않음 – 암호화되어 저장됨
  - **스마트폰 제조사별 백업 방식 상이**
    - 백업 데이터로부터 사용자 데이터를 복구하기 위해 제조사별로 백업 방식을 분석해야 함



데이터 암호화

- 백업 데이터 암호화 시나리오

- KDF(Key Derivation Function)
- PBKDF(Password Based KDF)

PIN 또는 패스워드 등
비밀 값 입력

비밀 값 기반 키 생성

백업 데이터 암호화

랜덤한 SALT

- PBKDF2-HMAC-SHA1
- PBKDF2-HMAC-SHA256
- SHA1
- SHA256 등…

키 = PBKDF(비밀 값, SALT, ITERATION)

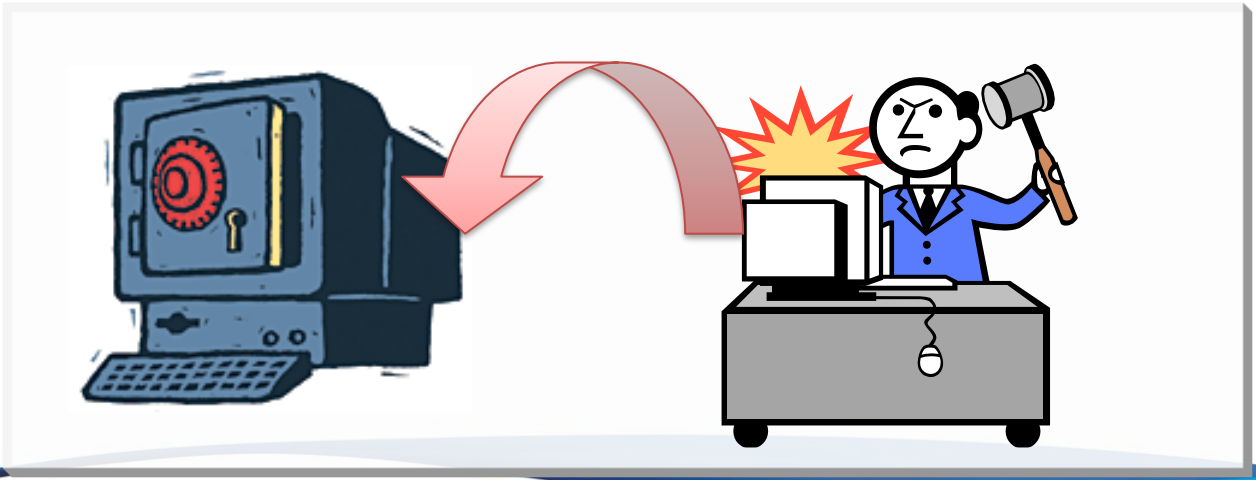
키 = HASH(비밀 값 || SALT)

- 블록암호 : AES, SEED 등
- 운영모드 : CBC, CTR 등
- 패딩 : PKCS#7Padding

암호문 =
블록암호-운영모드-패딩(평문, 키)

안티 포렌식 기술 대응방안

- **Anti-Forensic에 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