안티안티 포렌식

JK Kim

@pr0neer

forensic-proof.com

proneer@gmail.com

개요

1. 안티안티 포렌식 소개
2. 데이터 파괴 기법
3. 데이터 변형 기법
4. 데이터 은닉 기법
5. 데이터 조작 기법
6. 흔적 최소화 기법

안티안티 포렌식 소개

안티 포렌식

- **안티 포렌식**
  - 자신에게 불리하게 작용할 가능성이 있는 증거물을 훼손하거나 차단하는 일련의 행위

- **안티 포렌식의 목적**
  - 탐지를 회피하거나 정보 수집 방해
  - 조사관의 분석 시간을 증가
  - 디지털포렌식 도구의 실행을 방해하거나 오류를 발생시킴
  - 아티팩트가 남지 않도록 로깅을 차단하거나 우회
  - 증거로서 가치가 없도록 증거를 훼손

- **안티 포렌식 기법**
  - 데이터 파괴 기법, 데이터 변형 기법, 데이터 은닉 기법, 데이터 조작 기법 등

안티 포렌식 vs 정보보호

- **안티 포렌식**
  - 조사를 방해하기 위해 증거가 될 수 있는 데이터를 의도적으로 파괴

- **정보보호**
  - 사용자 혹은 기업 입장에서 기밀 데이터 혹은 개인정보보호를 위해 정당한 파괴

- 같은 기법이라도 **사안에 따라 안티 포렌식 기법이 되거나 정보보호 기법**이 될 수 있음

안티안티 포렌식

- **안티안티 포렌식**
  - 안티 포렌식 기법에 대응하기 위한 기법

- **안티안티 포렌식 기법**
  - 데이터 복구 기법
  - 암호 공격 기법
  - 은닉 데이터 탐지 기법
  - 추가적인 아티팩트에 대한 연구
  - 아티팩트 통합 분석

데이터 파괴 기법

데이터 파괴 기법

1. 파일/폴더 삭제
2. 레코드 삭제
3. 사용 흔적 삭제 도구
4. 파일시스템 포맷
5. 소프트웨어 기반 완전삭제(Wiping)
6. 하드웨어 기반 완전삭제(Wiping)
7. 스마트기기 공장 초기화

데이터 파괴 기법

1. 파일/폴더 삭제

- **휴지통 삭제**
  - Delete 키를 이용한 삭제
  - 삭제할 경우 휴지통으로 이동

- **바로 삭제 (휴지통 우회)**
  - Shift + Delete 키를 이용한 삭제
  - 삭제할 경우 휴지통을 거치지 않고 바로 삭제

1. 파일/폴더 삭제

▪ 휴지통 삭제

- 파일을 삭제할 경우 해당 파일의 MFT 레코드(NTFS 경우) 삭제
- 휴지통 폴더의 새로운 파일 이름으로 MFT 레코드 생성
- 결과적으로,
  - ✓ 파일 삭제 시 파일 메타 정보의 변경만 일어나고 파일 내용(데이터 영역)은 변화 없음
  - ✓ 파일에 대한 메타데이터가 2개 생성(원본 메타데이터, 휴지통 파일의 메타데이터)

- **운영체제 별 휴지통 폴더**

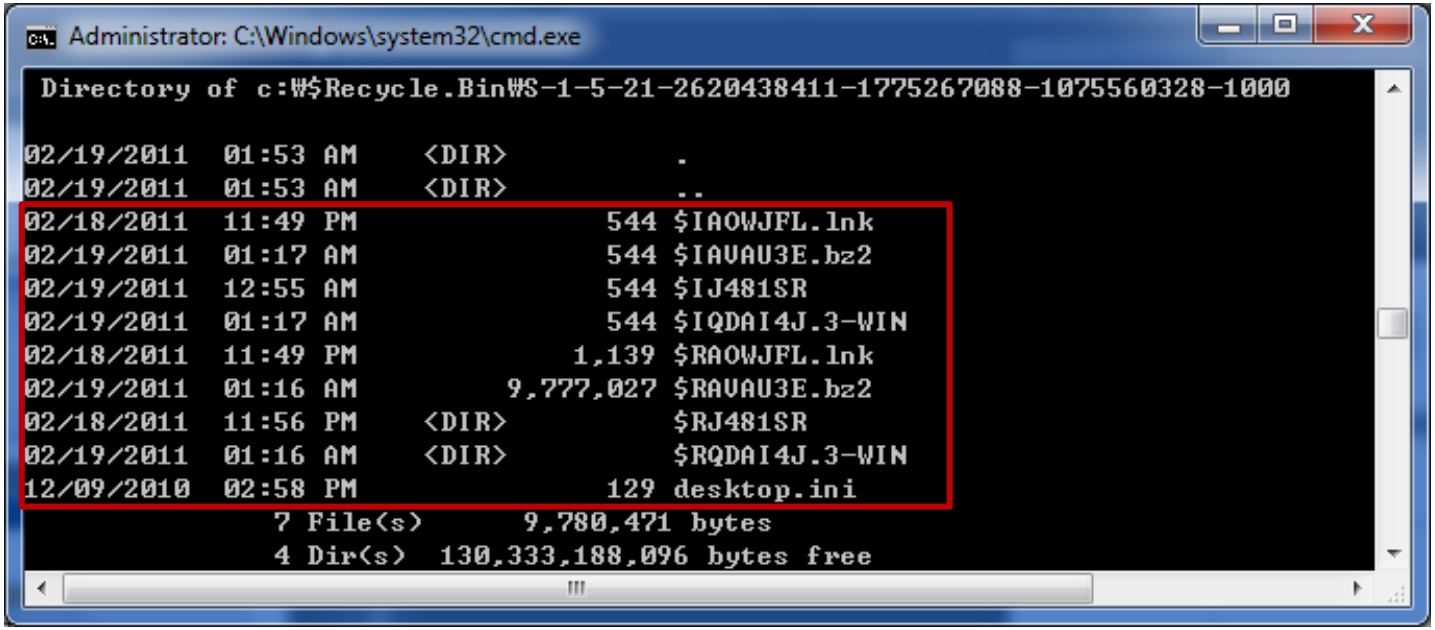
운영체제	기본 파일 시스템	휴지통 폴더
윈도우 9x/ME	FAT32	<volume>₩Recycled₩
윈도우 NT/2K/XP	NTFS	<volume>₩Recycler₩<USER_SID>₩
윈도우 Vista/7	NTFS	<volume>₩$Recycle.Bin₩<USER_SID>₩

  - ✓ 각 볼륨마다 각 사용자 SID로 휴지통 관리

1. 파일/폴더 삭제

▪ 휴지통 삭제

• 윈도우 Vista 이후의 휴지통



✓ **$R [임의문자열].[원본확장자]**

- 삭제된 파일의 데이터

✓ **$I [임의문자열].[원본확장자]**

- 파일의 삭제 정보(원본 경로, 삭제 시간 등)

1. 파일/폴더 삭제

▪ 휴지통 삭제

• $I 파일 구조

✓ 고정된 554 바이트 크기로 삭제된 파일마다 하나씩 생성

범위	크기	설명
0 – 7	8 bytes	파일 헤더
8 – 15	8 bytes	원본 파일 크기
16 – 23	8 bytes	삭제된 파일 시간 정보 (Windows 64-bit Timestamp, FILETIME)
24 – 543	520 bytes	원본 파일 경로 (UNICODE)

데이터 파괴 기법

1. 파일/폴더 삭제

- **휴지통 삭제 ➔ 대응**
  - 휴지통으로 이동한 경우, $I 파일로 삭제 정보 확인
  - 휴지통 비우기를 한 경우, $R 파일명 패턴을 가지는 MFT 레코드를 획득하여 삭제 파일 복원
  - 휴지통 비우기를 한 경우, $I 파일명 패턴을 가지는 MFT 레코드를 획득하여 삭제 정보 파일 복원
  - 휴지통 비우기를 한 경우, 삭제된 파일 형식에 기반하여 파일 카빙 복구
  - 휴지통 비우기를 한 경우, $I 파일을 카빙 복구하여 삭제 파일 정보 획득

1. 파일/폴더 삭제

- **# 실습 – 실습 시스템의 휴지통 흔적 분석하기!!**

1. 파일을 일반 삭제 후, 휴지통 흔적 분석하기

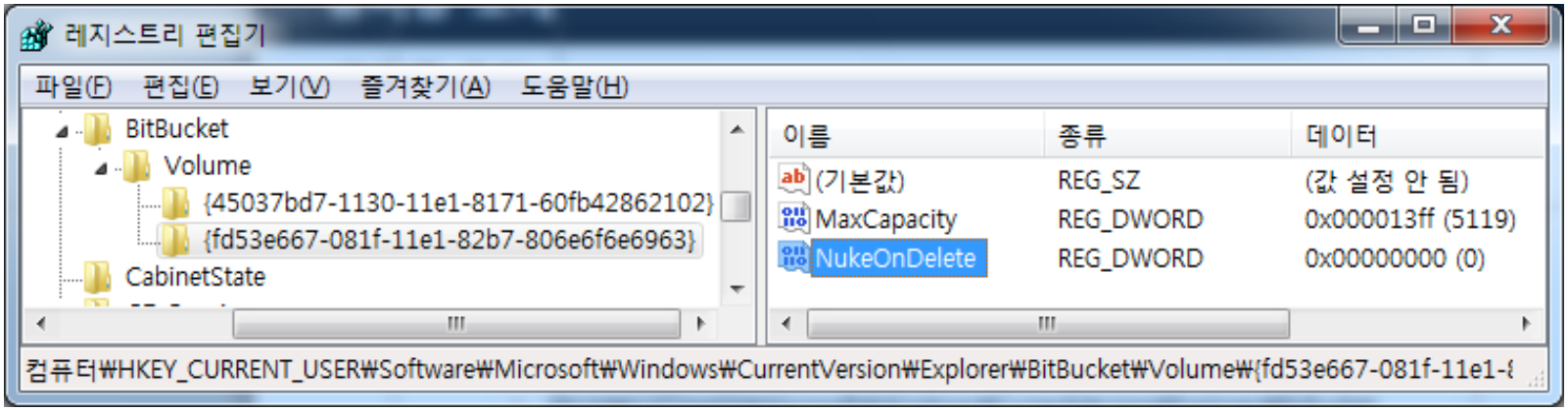
2. 휴지통 비우기를 한 후, 파일 카빙으로 $I 파일을 복구하여 분석하기

1. 파일/폴더 삭제

▪ 바로 삭제

- **휴지통을 우회하여 삭제하는 방법**

1. SHIFT 키 + DELETE 키
2. "NukeOnDelete " 레지스트리 값 설정
   - HKU₩{USER}₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩**Bitbucket₩Volume₩{GUID}**



- **휴지통을 우회할 경우 흔적**

✓ 대상 파일/폴더 메타정보의 삭제 플래그 세팅(해당 메타정보는 다른 파일 정보로 덮어써질 수 있음)

✓ 대상 파일의 데이터는 비할당 영역으로 변경(해당 데이터는 다른 파일 데이터로 덮어써질 수 있음)

1. 파일/폴더 삭제

- **바로 삭제 ➔ 대응**
  - 파일시스템 메타데이터($MFT)에서 삭제 플래그가 세팅된 파일만 추출하여 복구
  - 비할당 영역에서 파일 형식에 기반하여 파일 카빙 복구

  - **파일 카빙 기법** – http://forensic-proof.com/slides (데이터 복구의 거의 모든 것)
    - ✓ **연속적인 카빙 ➔** 데이터가 연속된 공간에 저장된 경우
      - 헤더/푸터 카빙
      - 램 슬랙 카빙
      - 파일 크기 카빙
      - 파일 검증 카빙
    - ✓ **비연속적인 카빙 ➔** 데이터가 단편화되어 조각나 저장된 경우
      - 시그니처 이용
      - 엔트로피 이용
      - 바이트 분포/편차 이용
      - ASCII 빈도 수 이용
      - 공통된 패턴 이용

2. 레코드 삭제

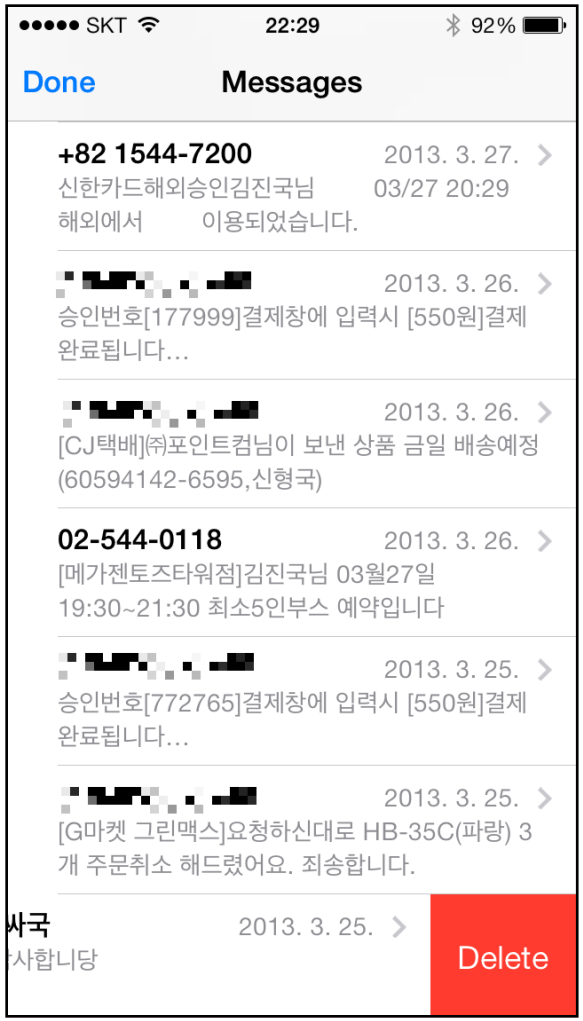
▪ 레코드 삭제 유형

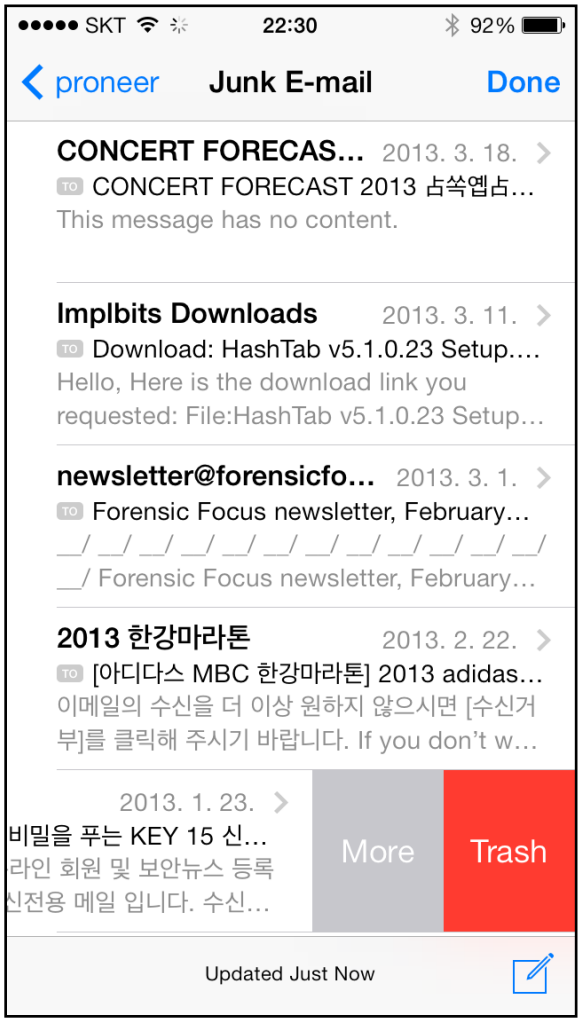
- 데이터베이스와 같은 형식을 가지는 경우 특정 레코드만 삭제 가능

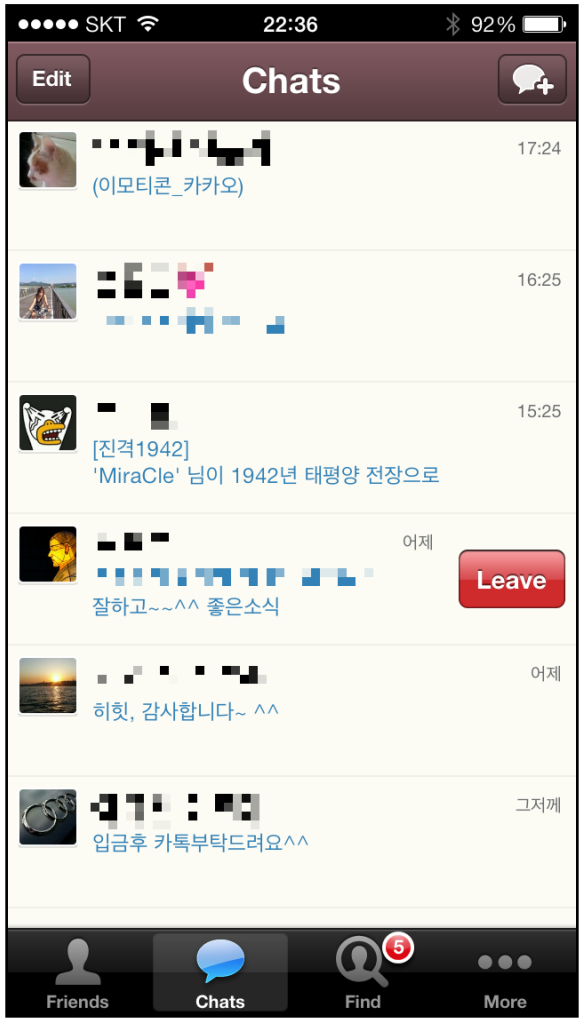
- **레코드 삭제 지원**
  - ✓ 데이터베이스 (MS SQL, Oracle, My SQL, SQLite 등)
  - ✓ 스마트폰의 채팅, 문자, 통화목록 등 (SQLite, Plist 등)
  - ✓ 메일 스토리지 파일 (PST, DBX, OST, MBOX 등)

2. 레코드 삭제

- 레코드 삭제 예제

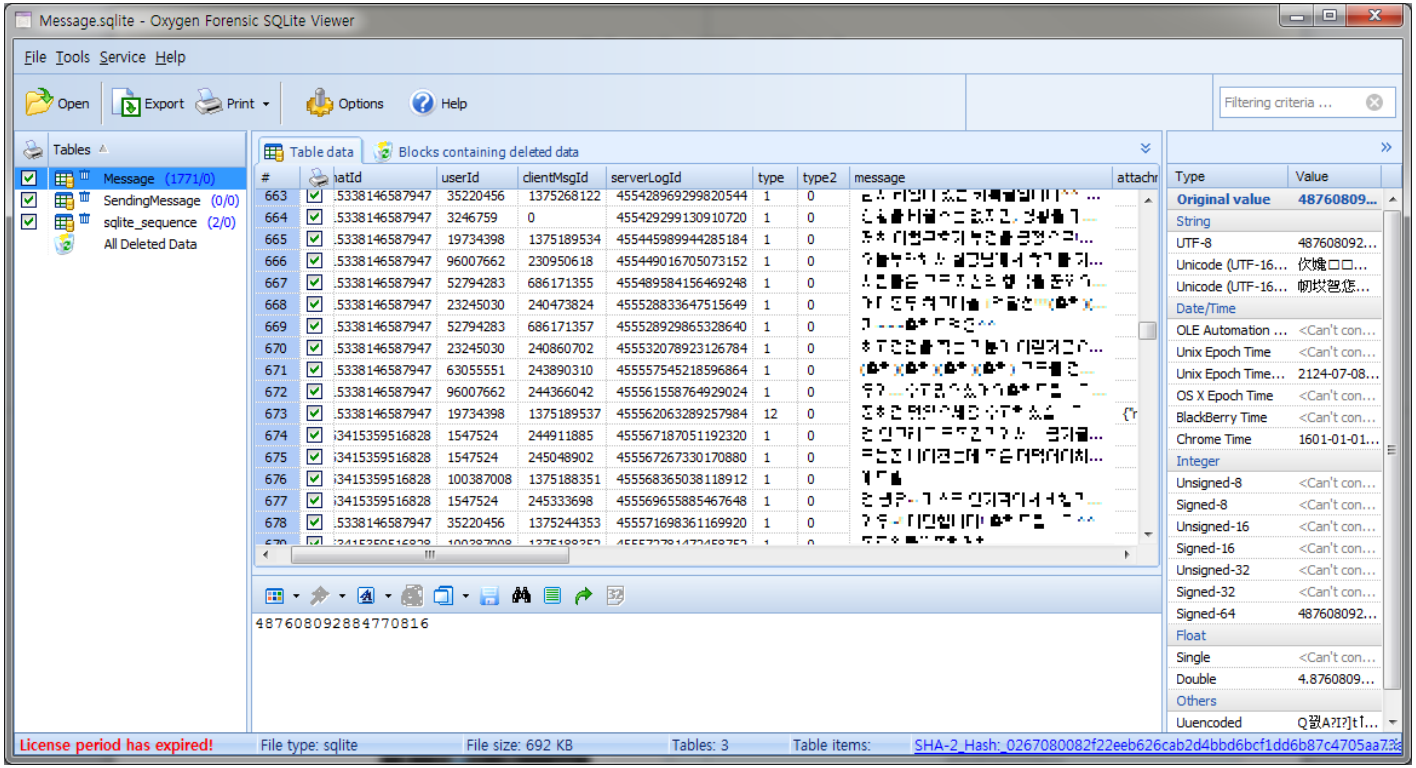






2. 레코드 삭제

- **레코드 삭제 ➔ 대응**
  - 대부분의 레코드 지원 구조는 파일시스템과 마찬가지로 레코드를 완전 삭제하지 않음
  - 파일 형식을 분석하여 비할당 영역에서 삭제된 레코드 복원 ➔ 고급 기술 필요
  - 상용 데이터베이스 복원 도구나 메일 복원 도구 사용



2. 레코드 삭제

- # 실습 – SQLite 레코드 삭제 후 복구하기!!

3. 사용 흔적 삭제

- **일반적인 시스템/사용자 아티팩트**
  - 최근 접근 문서(Recent)
  - 각 응용프로그램 MRU 정보
  - 썸네일/아이콘 캐시
  - 점프 목록
  - 프리패치
  - 웹 브라우저 사용 흔적
  - 이벤트 로그
  - … …

3. 사용 흔적 삭제

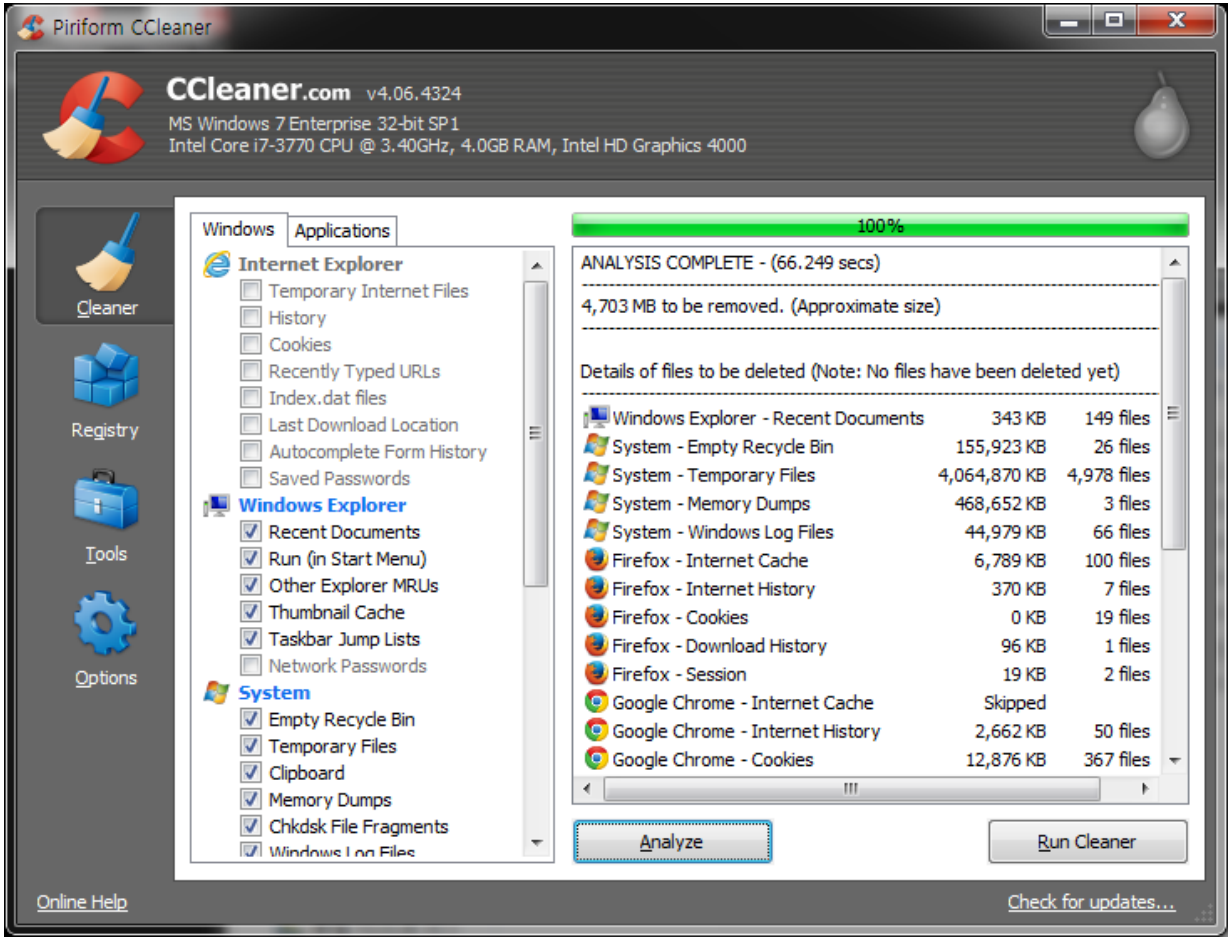
▪ 사용 흔적 삭제 도구

- 디지털 포렌식 분석의 기본이 되는 데이터를 일괄/선택 삭제 지원

- **대표적인 사용 흔적 삭제 도구 (최적화 프로그램)**
  - ✓ **CCleaner** – http://www.piriform.com/ccleaner/download
  - ✓ **CleanAfterMe** – http://www.nirsoft.net/utils/clean_after_me.html
  - ✓ **EasyCleaner** – http://personal.inet.fi/business/toniarts/ecleane.htm
  - ✓ **Moo0 Disk Cleaner** – http://www.moo0.com/
  - ✓ **CacheMan** – http://www.outertech.com/en/why-is-my-computer-so-slow
  - ✓ **고클린** – http://www.gobest.co.kr/goclean/goclean1.htm
  - ✓ **울타리** – http://rodream.net/index.htm?page=safefence
  - ✓ **다음 클리너** – http://cleaner.daum.net/
  - ✓ **별클리너** – http://nac.startools.co.kr/home/starcleaner/starcleaner.html

3. 사용 흔적 삭제

- 사용 흔적 삭제 도구
  - CCleaner



3. 사용 흔적 삭제

- **사용 흔적 삭제 도구 ➔ 대응**
  - 도구 설치 및 사용 흔적 조사
  - 의도적인 행위인지 파악
  - 도구에서 지원하는 아티팩트와 삭제 방식을 테스트
  - 복구가 가능한 경우 최대한 복구하여 분석

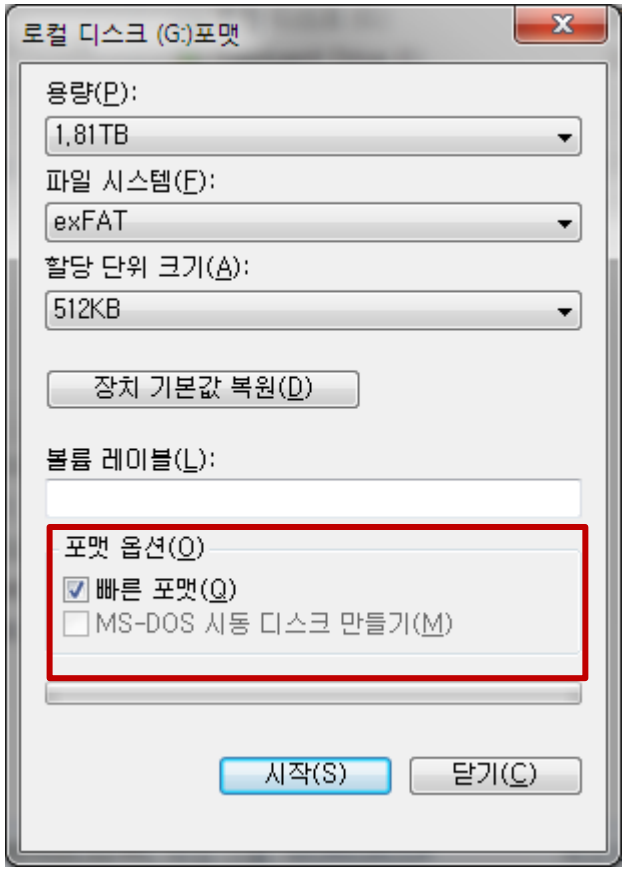
3. 사용 흔적 삭제

- **# 실습 – CCleaner 설치 및 실행 아티팩트 분석하기!!**

1. CCleaner 설치/삭제 후 아티팩트의 변화 살펴보기
2. CCleaner 삭제 방식 분석하기

4. 파일시스템 포맷

- **빠른 포맷 vs 일반 포맷**
  - **윈도우 Vista 이전**
    - ✓ 빠른 포맷은 볼륨의 첫 구조적 데이터만 생성
    - ✓ 일반 포맷은 빠른 포맷 + 디스크 체크
  - **윈도우 7 이후**
    - ✓ 빠른 포맷은 볼륨의 첫 구조적 데이터만 생성
    - ✓ 일반 포맷은 전체 볼륨 초기화(0으로 덮어쓰기)



4. 파일시스템 포맷

- **빠른 포맷 vs 일반 포맷 ➔ 대응**
  - **완전 삭제를 하지 않은 경우**
    - ✓ 주요 파일시스템 메타데이터만 손상
    - ✓ 나머지 메타데이터를 이용해 파일시스템 정상 데이터 획득 가능
  - **완전 삭제를 한 경우**
    - ✓ 데이터 복구 불가능
    - ✓ 다른 증거물에서 증거 획득

4. 파일시스템 포맷

- **# 실습 – 실습 시스템에서 포맷 후 파일시스템 변화 분석하기!!**

1. 빠른 포맷 후 파일시스템 변화 분석하기
2. 일반 포맷 후 파일시스템 변화 분석하기

5. 소프트웨어 기반의 완전 삭제

▪ 소프트웨어를 이용한 완전 삭제 방법

- **덮어쓰기**
  - ✓ 삭제하고자 하는 데이터에 [0, 1, Random]를 덮어씀
  - ✓ 파일 데이터 뿐만 아니라 메타 정보도 필수 고려
  - ✓ 복구 가능성은,
    - 개별 비트의 복구 가능성은 있지만 포렌식적으로 유효한 데이터의 복구 가능성은 거의 없음
    - 최소 1번 ~ 2번(패턴, 보수패턴) 덮어쓰기 필요

- **암호화**
  - ✓ 관용 암호화 기법을 이용해 안전하게 파일 혹은 디스크 암호화

5. 소프트웨어 기반의 완전 삭제

▪ 소프트웨어를 이용한 완전 삭제 방법

• 덮어쓰기 기반의 영구 삭제 표준

표준	년도	반복	패턴	비고
U.S. Navy	1993	3	문자, 보수, 랜덤	검증 필수
U.S. Air Force	1996	4	0, 1, 문자	검증 필수
Peter Gutmann	1996	1-35	매우 다양	원래 현재는 사용되지 않는 MFM, RLL을 위해
Bruce Schneier	1996	7	0, 1, 5번의 유사 랜덤	-
U.S. DoD	2001	3	문자, 보수, 다른 패턴	-
German Federal	2004	2-3	불규칙 패턴, 보수	-
CSEC	2006	3	0(1), 보수	분류되지 않은 매체를 위해
NIST	2006	1	?	-
U.S. NISP	2006	?	?	더 이상 지정하지 않음
NSA/CSS	2007	0	?	디가우즈 또는 파괴
Australian	2008	1	?	디가우즈 또는 일급 비밀 매체 파괴
New Zealand	2008	1	?	기밀 데이터를 위해

5. 소프트웨어 기반의 완전 삭제

- 덮어쓰기 기반의 완전 삭제 소프트웨어
  - **Eraser** – http://eraser.heidi.ie/
  - **Moo0 FileShredder 1.18** – http://www.moo0.com/
  - **Moo0 Anti-Recovery 1.06** – http://www.moo0.com/
  - **R-Wipe & Clean** – http://www.r-wipe.com/ko/
  - **WipeDrive** – https://www.whitecanyon.com/ConsumerWipeDrive
  - **SecureClean** – https://www.whitecanyon.com/ConsumerSecureClean
  - **QuickWiper –** http://www.quickwiper.com/
  - **FINALeRASER –** http://www.finaldata.co.kr/Products/?s=PRD&c=19
  - **ViRobot DataEraser –** http://shop.hauri.co.kr/product/product_detail.html?ProdCode=MTk=

5. 소프트웨어 기반의 완전 삭제

- **소프트웨어를 이용한 완전 삭제 방법 ➔ 대응**
  - 1번만이라도 덮어쓰기가 정확히 이루어졌다면 현실적으로 복구 불가능
  - 다른 증거물에서 관련 증거 획득

5. 소프트웨어 기반의 완전 삭제

- **# 실습 – Moo0의 File Shredder로 파일 삭제 후 변화 분석하기!!**

1. File Shredder 설치 후 예제 파일 삭제
2. 파일의 메타정보와 데이터의 변화 분석하기

6. 하드웨어 기반의 완전 삭제

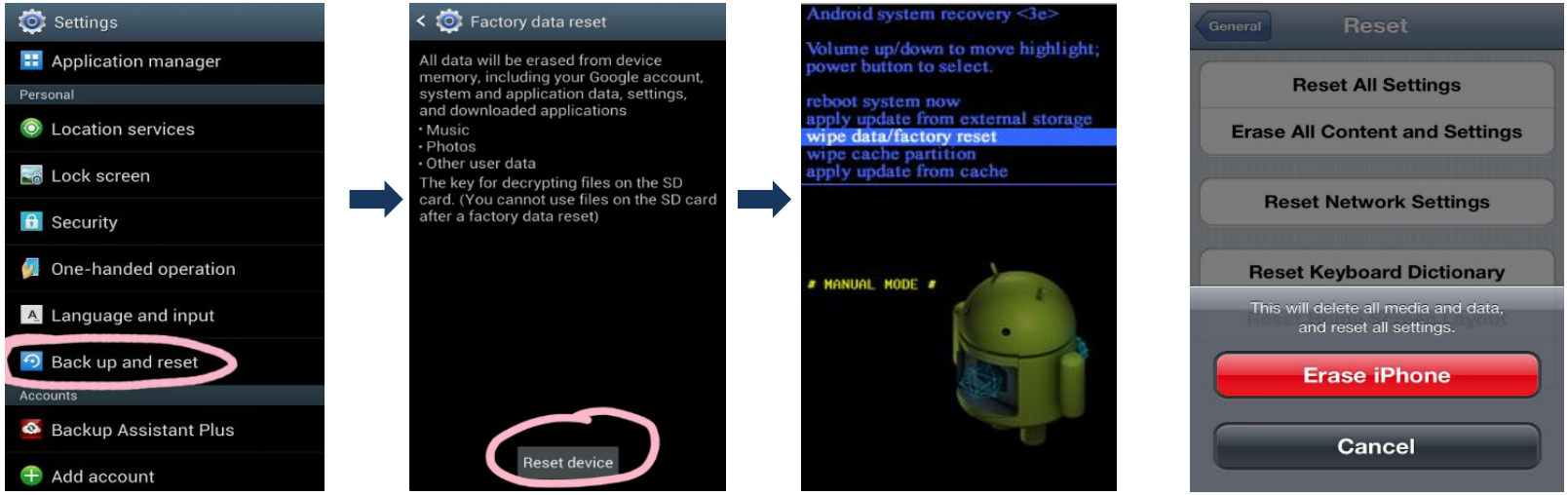
- **하드웨어를 이용한 완전 삭제 방법**
  - **디가우징(Degaussing)**
    - ✓ 강한 자기장을 노출시켜 자기디스크의 표면의 자력 흐름 파괴
  - **물리적 천공, 파쇄**
    - ✓ 강력한 하드웨어 기계를 사용해 물리적으로 구멍을 내거나 파쇄

6. 하드웨어 기반의 완전 삭제

- **하드웨어를 이용한 완전 삭제 방법 ➔ 대응**
  - **디가우징(Degaussing)**
    - ✓ 디가우징되었다면 기술적으로 복구 불가능
  - **물리적 천공, 파쇄**
    - ✓ 천공 또는 파쇄가 되면 기술적으로 복구 불가능

7. 스마트기기의 공장 초기화

- **스마트기기 초기화 방법**
  - **안드로이드**
    - ✓ 안드로이드 4.0 아이스크림 샌드위치 이전 – 비할당 영역에서 데이터 복구 가능
    - ✓ 안드로이드 4.1 젤리빈 이후 – 플래시 메모리 전체를 초기화하여 복구 불가능
  - **아이폰**
    - ✓ 하드웨어 기반의 암호화 기능으로 모든 데이터가 암호화되어 저장
    - ✓ 사용자 키를 모른다면 복구 불가능



안드로이드 공장 초기화 아이폰 공장 초기화

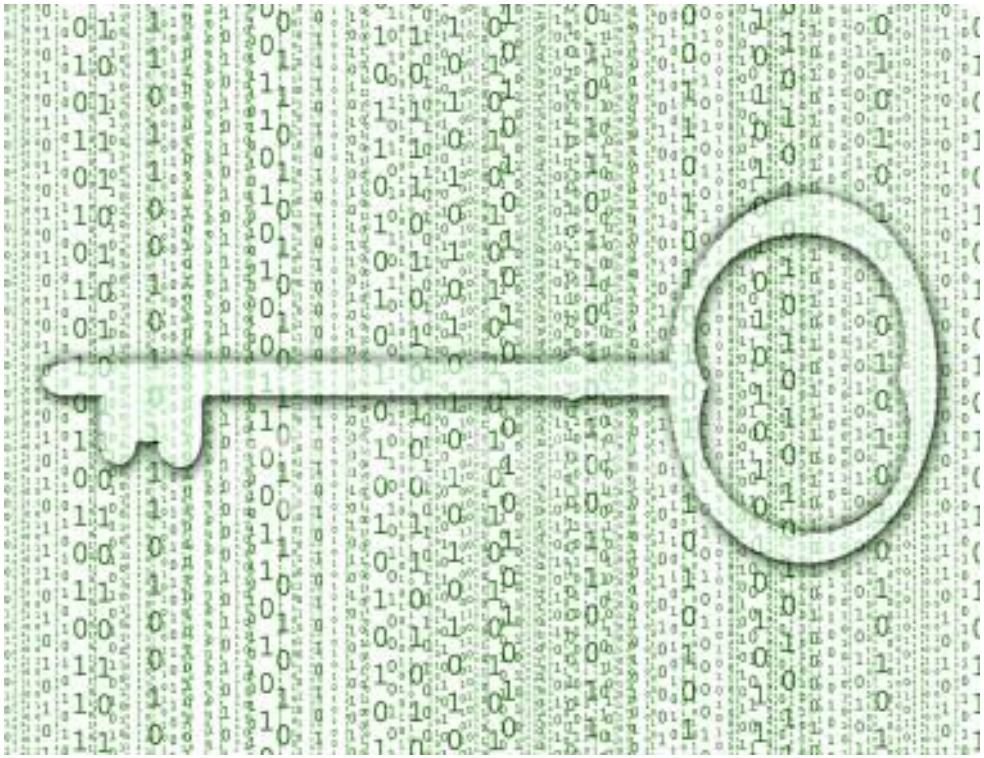
7. 스마트기기의 공장 초기화

- **스마트기기 초기화 방법 ➔ 대응**
  - **안드로이드**
    - ✓ 젤리빈 이상이라면 플래시 영역은 포기
    - ✓ SD 카드, 클라우드 백업, 로컬 백업 영역에서 흔적 조사
  - **아이폰**
    - ✓ 4자리 비밀번호가 설정되어 있다면 접근 불가
    - ✓ 비밀번호를 알거나 없다면 백업 프로토콜을 이용해 제한된 분석
    - ✓ 클라우드 백업, 로컬 백업 영역에서 흔적 조사

데이터 변형 기법

데이터 변형 기법

1. 인코딩 기법
2. 난독화 기법
3. 실행 압축 기법
4. 암호화 기법



데이터 변형 기법

1. 인코딩 기법

- **인코딩**
  - 정보의 형태나 형식을 다른 형태나 형식으로 변환하는 처리 혹은 처리 방식

- **인코딩 목적**
  - 표준화
  - 보안
  - 처리속도 향상
  - 저장 공간 절약

- **대표 인코딩**
  - 문자 인코딩 (ASCII, ISO 8859, CP949, EUC-KR, UTF-7, UTF-8 등)
  - Base64 인코딩 ➔ 바이너리 데이터를 문자 코드에 영향을 받지 않는 ASCII 영역 문자로 변환
  - 퍼센트 인코딩 ➔ URI 에서 문자를 표현하기 위한 인코딩
  - 신호 처리 분야에서도 다양한 인코딩/부호화 기법 사용 ➔ 포렌식 분석의 고려대상은 아님

1. 인코딩 기법

- **인코딩 ➔ 대응**
  - 분석 아티팩트에 따라 다양한 인코딩 방법 사용
  - 각 아티팩트 분석 시 가독성이 있도록 디코딩하여 표현
  - 예제
    - ✓ 레지스트리 ROT-13 인코딩
    - ✓ 웹 브라우저 흔적 URL 인코딩
    - ✓ 한글 관련 데이터의 한글 인코딩
    - ✓ 이메일 데이터의 Base64 인코딩

2. 난독화 기법

- **난독화**
  - 프로그래밍 언어로 작성된 코드나 바이너리를 분석이 어렵게 만드는 작업

- **대표 난독화**
  - URL 난독화
  - 자바스크립트 난독화
  - 가상화 코드 난독화 (코드 가상화)

2. 난독화 기법

- **난독화 ➔ 대응**
  - 널리 알려진 방법 이외에 매뉴얼한 방법이 자주 사용
  - 분석 과정에서 난독화된 코드나 바이너리는 디코딩해주는 루틴을 찾아 분석
  - 노하우와 끈기가 필요!!

3. 실행 압축 기법

- **실행 압축**
  - 실행 파일을 압축하는 기술로 패킹(Packing)이라는 용어로 불림

- **실행 압축 목적**
  - 코드 보호
  - 처리 효율 ➔ 용량을 줄인 코드의 전송 (저장장치 속도 vs 프로세서 속도)
  - 저장 공간 효율 (임베디드 장치)

- **대표 실행 압축 기법**
  - UPX, ASPack, ASProtect, PECompat, PE-Crypt, PElockNT, FSG, Armadillo
  - Themida, VMProtect, Enigma

3. 실행 압축 기법

- **실행 압축 ➔ 대응**
  - 단순 실행 압축 기법의 경우, 자동화된 언팩(Unpack) 기법 사용
  - 고급 실행 압축 기법이나 매뉴얼(커스텀) 기법의 경우, 언팩 루틴을 찾아 끈기를 가지고 도전!!
  - 다수의 중복 실행 압축 기술을 사용할 경우, 자동으로 악성코드로 진단

4. 암호화 기법

- **암호화**
  - 알고리즘을 이용하여 정보를 확인할 수 없도록 변형
  - 원래 정보로 되돌리는 복호화 가능

- **대표적인 암호화 알고리즘**
  - **대칭키**
    - ✓ 암/복호화 키가 동일
    - ✓ DES, TDES, AES, SEED, ARIA 등
    - ✓ 주로 파일이나 디스크 암호화에 사용
  - **비대칭키(공개키)**
    - ✓ 암/복호화 키가 다름
    - ✓ D-H(Diffie-Hellman), RSA, ElGamal, ECC
    - ✓ 주로 디지털 서명이나 PKI 구조에 사용

4. 암호화 기법

- **암호화 알고리즘 활용**
  - **응용프로그램 암호화** : 문서, 압축, 데이터베이스, 이메일 등
  - **인증 토큰 암호화** : 윈도우/리눅스 로그인, 안드로이드/iOS 로그인 등
  - **디스크 암호화** : TrueCyprt, BitLocker, BestCrypt, FreeOTFE 등
  - **정보보호 솔루션** : DRM 등

4. 암호화 기법

- **암호화 ➔ 대응**
  - **암호 공격 기술**
    - ✓ 사회 공학
    - ✓ 사전 공격
    - ✓ 전수 조사
  - **공격 향상 기술**
    - ✓ 고속 연산 기술 (NVDIA Tesla, PS3 등)
    - ✓ 분산 처리 기술
  - 알려진 알고리즘 + 일정 길이 이상의 패스워드 사용 ➔ 전수 조사 공격으로 알기 어려움
    - ✓ 사회 공학이나 사전 공격에 집중

4. 암호화 기법

- # 실습 – 윈도우 패스워드 크랙하기!!

데이터 은닉 기법

데이터 은닉 기법

1. 데이터 구조 이용
2. 슬랙 영역 이용
3. 스테가노그래피 기법 이용

1. 데이터 구조 이용

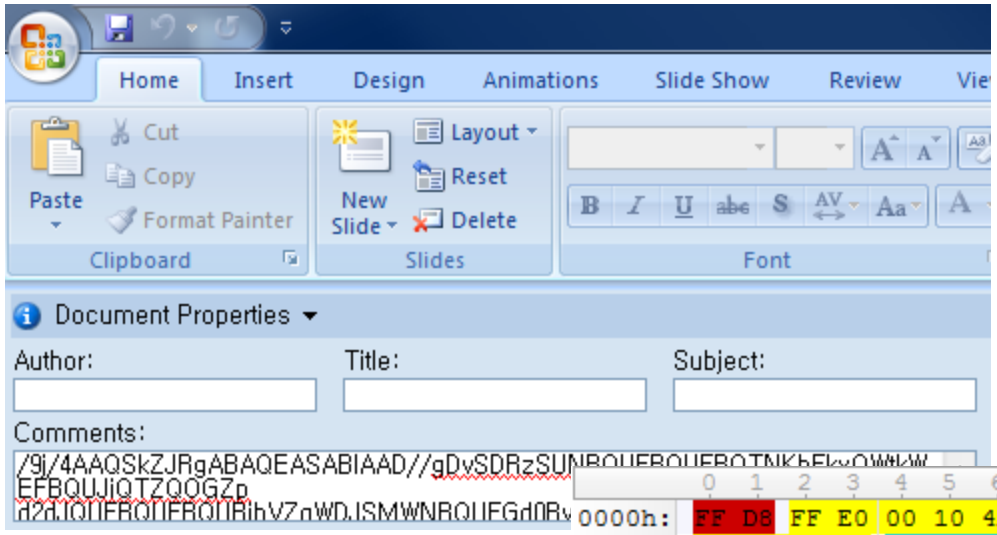
▪ 데이터 구조

- 파일 헤더 구조체의 사용되지 않는 영역에 데이터 은닉
- 파일 구조 변경을 통해 일반 파일 실행 시에는 은닉 데이터가 보이지 않도록 조작
- 파일의 속성 필드에 데이터 은닉
- 파일시스템 구조 상 낭비되는 영역에 데이터 은닉 (MFT Slack, ADS 등)

- **대응**
  - ✓ 데이터 구조에 사용되지 않는 필드 검증
  - ✓ 데이터 구조가 정상인지 검증

1. 데이터 구조 이용

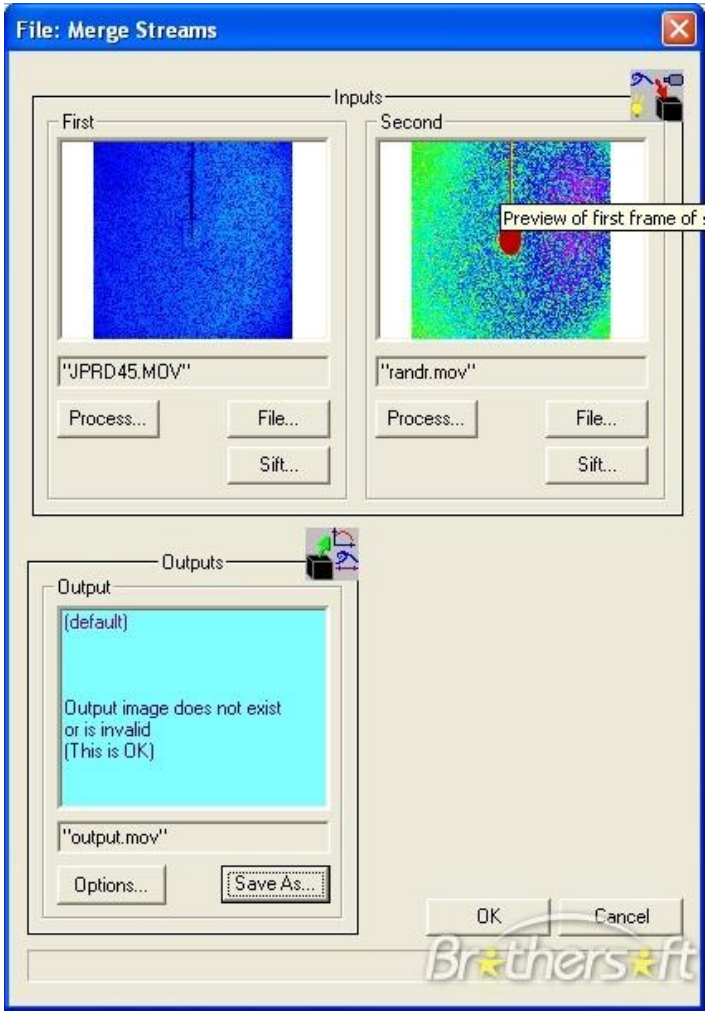
- **예제) DEFCON 18 CTF – Forensics 300,** http://forensic-proof.com/archives/495




```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 48   ÿØÿà..JFIF.....H
0010h: 00 48 00 00 FF DB 00 43 00 05 03 04 04 04 03 05   .H..ÿÛ.C........
0020h: 04 04 04 05 05 05 06 07 0C 08 07 07 07 07 0F 0B   ................
0030h: 0B 09 0C 11 0F 12 12 11 0F 11 11 13 16 1C 17 13   ................
0040h: 14 1A 15 11 11 18 21 18 1A 1D 1D 1F 1F 1F 13 17   ......!.........
0050h: 22 24 22 1E 24 1C 1E 1F 1E FF DB 00 43 01 05 05   "$".$....ÿÛ.C...
0060h: 05 07 06 07 0E 08 08 0E 1E 14 11 14 1E 1E 1E 1E   ................
0070h: 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E   ................
0080h: 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E   ................
0090h: 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E FF FE   ..............ÿþ
00A0h: 00 32 61 48 52 30 63 44 6F 76 4C 32 6C 79 59 33   .2aHR0cDovL2lyY3
00B0h: 42 70 59 33 4D 75 59 32 39 74 4C 32 6C 74 5A 79   BpY3MuY29tL2ltZy
00C0h: 35 77 61 48 41 2F 61 57 51 39 4D 54 55 34 4E 54   5waHA/aWQ9MTU4NT
00D0h: 67 4B FF C0 00 11 08 01 A7 01 C2 03 01 22 00 02   gKÿÀ....§.Â.."..
00E0h: 11 01 03 11 01 FF C4 00 1F 00 00 01 05 01 01 01   .....ÿÄ.........
```

1. 데이터 구조 이용

- **예제) Merge Streams** – http://merge-streams.softpile.com/



1. 데이터 구조 이용

- # 실습 – Merge Stream으로 Word, Excel 통합하기!!

2. 슬랙 영역 이용

▪ 슬랙 영역

- 물리적 구조와 논리적 구조의 차이로 발생하는 낭비되는 공간

- **슬랙 사용 유형**
  - ✓ **Slacker** : 파일 슬랙 공간에 데이터 은닉
  - ✓ **FragFS** : NTFS의 MFT에 데이터 은닉
  - ✓ **RuneFS** : 배드 블록에 데이터 은닉
  - ✓ **Waffen FS** : ext 저널 파일에 데이터 은닉
  - ✓ **KY FS** : 디렉터리 파일에 데이터 은닉
  - ✓ **Data Mule FS** : inode 예약된 공간에 데이터 은닉
  - ✓ **HPA, DCO** : HPA, DCO 영역에 데이터 은닉
  - ✓ 이 밖에 파일시스템 상에 존재하는 **슬랙 영역은 무궁무진!!!**

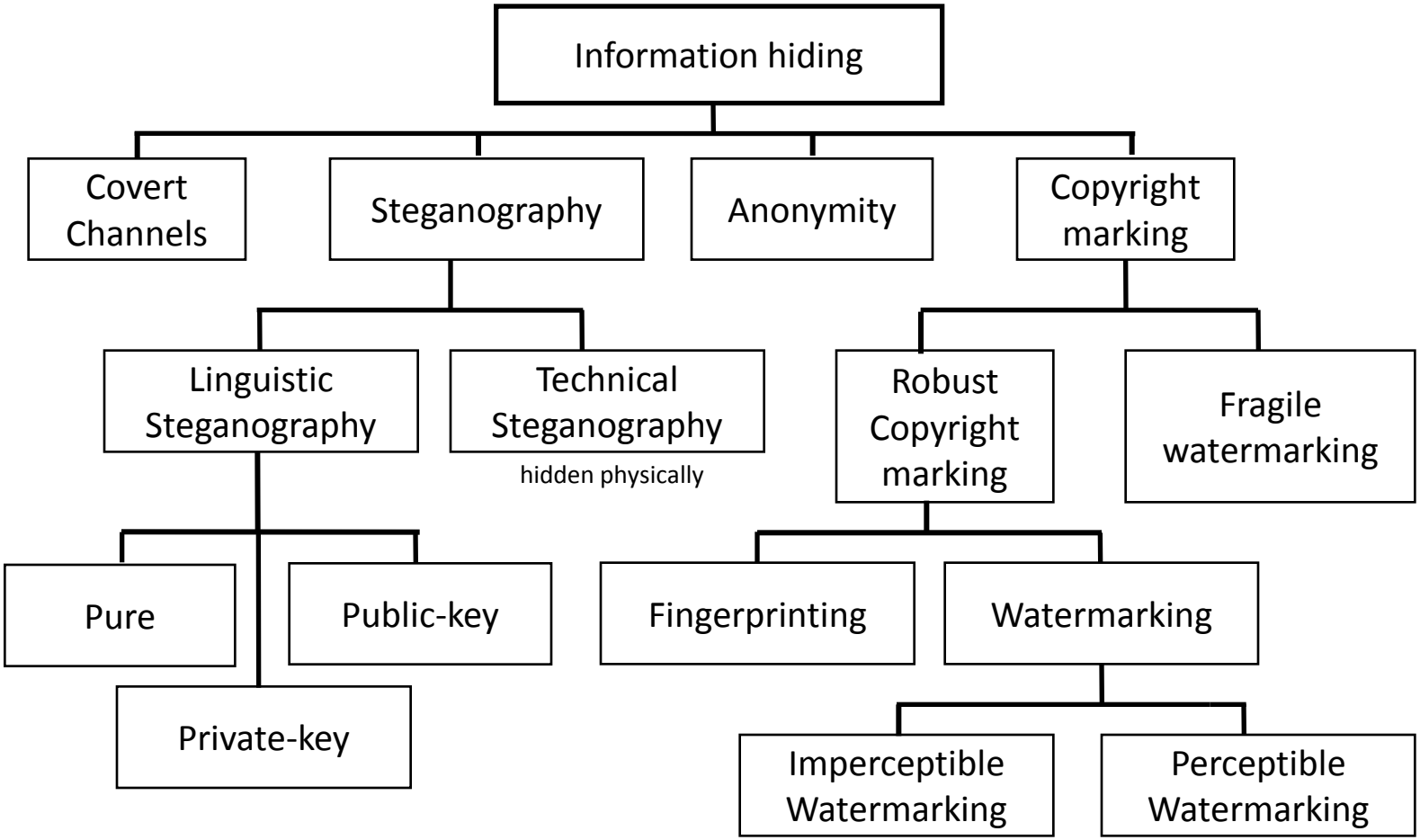
- **대응**
  - ✓ 슬랙 공간 검증

3. 스테가노그래피 기법 이용

- **스테가노그래피**
  - 비밀리에 전달하고자 하는 데이터는 은닉하고 비밀데이터의 존재자체도 숨기는 기법
  - 정보 은닉의 한 분야로 국내 학계에서는 "심층 암호"라는 용어로 사용
  - 그리스어에서 유래
    - ✓ Steganos(covered) + graphos(writing) ➔ "Covered Writing"

3. 스테가노그래피 기법 이용

- 정보 은닉 기술 분류



3. 스테가노그래피 기법 이용

- **아크로스틱(Acrostics) 스테가노그래피**
  - 1차 세계대전에서 사용
  - **샘플)** 독일 스파이가 전송한 메시지

> **"Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils".**

> **"Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils".**

➔ 각 단어의 2번째 문자를 조합 : "**pershing sails from NY June I**"

3. 스테가노그래피 기법 이용

- **텍스트(Text) 스테가노그래피**

정이 확 떨어진다

정말 너 같은 사람이랑 사귄 거 후회해

너랑 끝이다

알아서 이해해라

잘 지내

정이확떨어진다정

말너같은사람이랑

사귄거후회해너

랑끝이다알아서이

해해라잘지내

3. 스테가노그래피 기법 이용

- 이미지(image) 스테가노그래피

Cover-image

Stego-image (70,000 byte)

3. 스테가노그래피 기법 이용

- **이미지(image) 스테가노그래피**
  - 영상데이터 ➔ 잉여 정보가 많음
  - 영상데이터의 하위 비트가 변해도 시각적으로 감지하기 어려움
  - **예제) 하위 비트 변경**

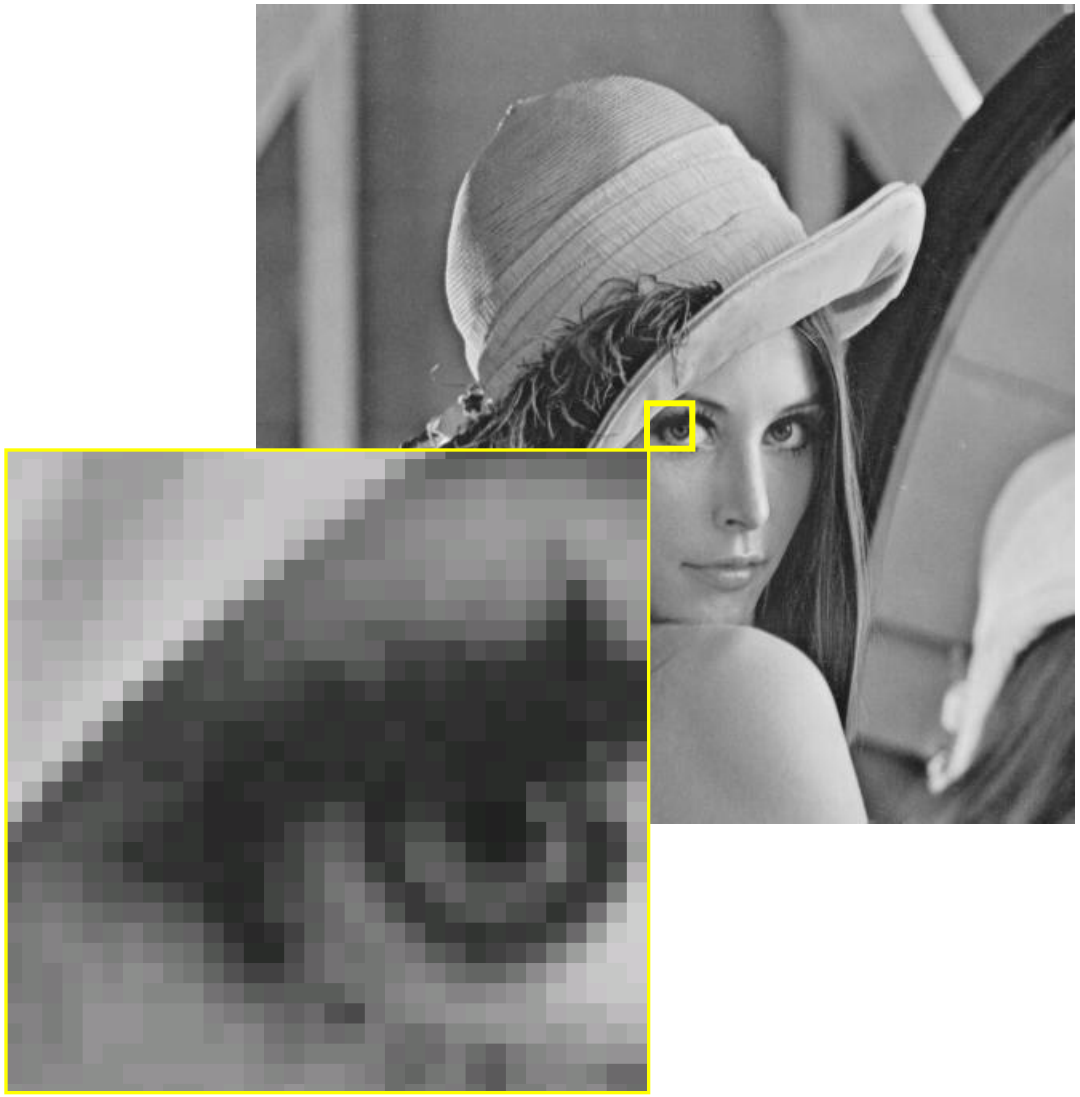
3. 스테가노그래피 기법 이용

▪ 이미지(image) 스테가노그래피

- **이미지 파일 형식**
  - ✓ 레스터(RAW) 형식 – 8비트 그레이스케일과 24비트 트루 컬러
    - BMP, PGM, PPM, RAS, TIFF
  - ✓ 팔레트 형식 – 8비트 인덱스 매칭 컬러
    - GIF, PNG, BMP
  - ✓ 손실 압축 형식 – DCT, DWT 기반
    - JPEG, JPEG2000
- **그 밖에 형식**
  - ✓ 벡터 형식 – WMF
  - ✓ 프린팅 형식 – PS, PDF

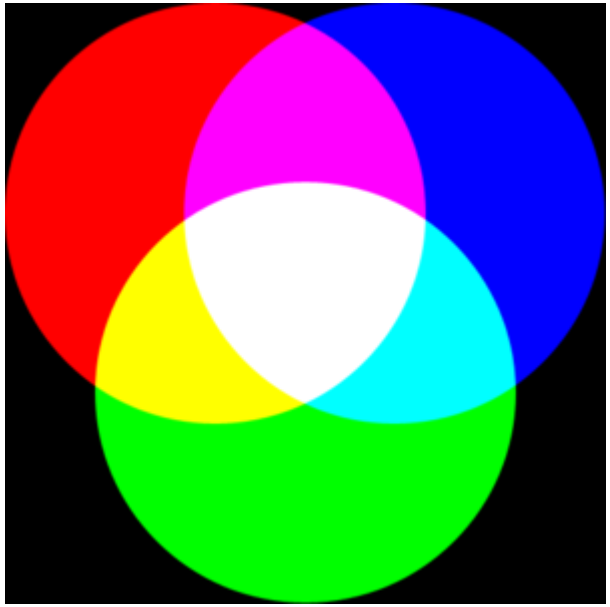
3. 스테가노그래피 기법 이용

- **이미지(image) 스테가노그래피**
  - **디지털 이미지**
    - ✓ 2 X 2 매트릭스
    - ✓ 픽셀 단위
    - ✓ 너비(width), 높이(height) 정보
  - **그레이스케일 이미지**
    - ✓ 하나의 픽셀을 광도에 따라 256레벨로 표현
    - ✓ 1 픽셀 = 8비트



3. 스테가노그래피 기법 이용

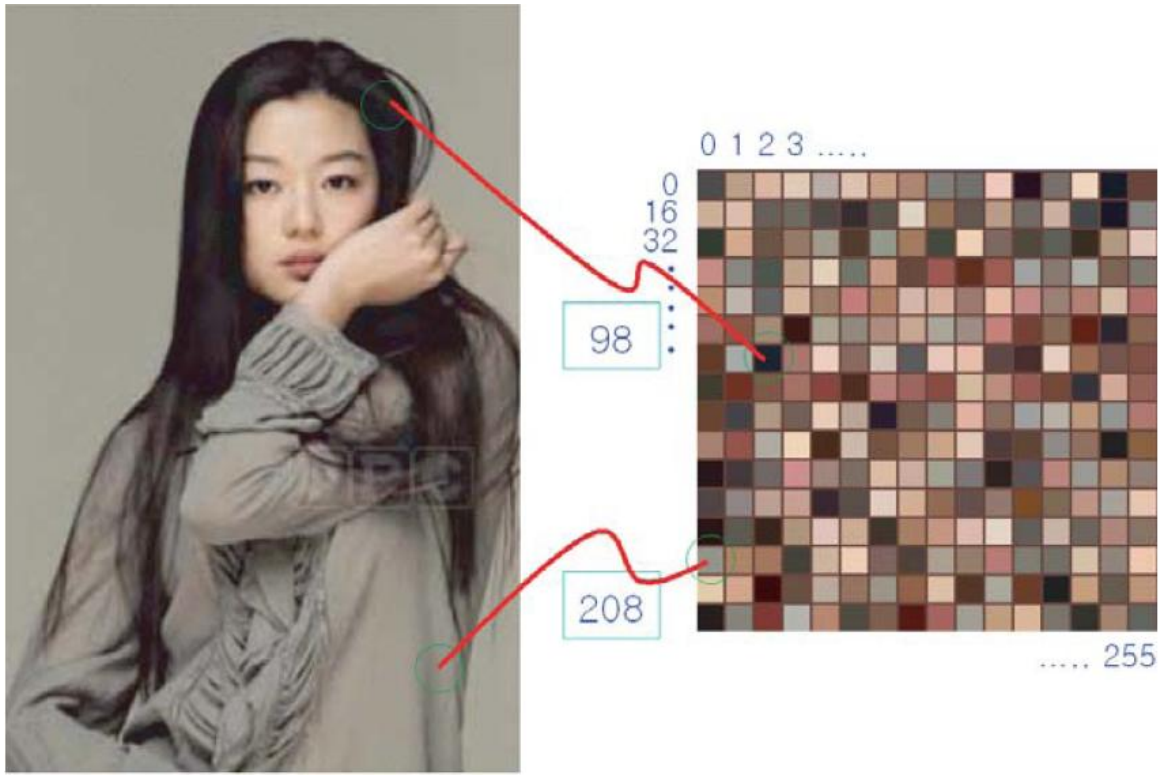
- **이미지(image) 스테가노그래피**
  - **트루컬러(또는 RGB) 이미지**
    - ✓ 1픽셀 = 빨강(Red) + 초록(Green) + 파랑(Blue)
    - ✓ 각 컴포넌트는 8비트로 표현
    - ✓ 1픽셀 = 24비트
    - ✓ RGB 이미지는 분석을 위해 그레이스케일로 변환 가능



A representation of additive color mixing

3. 스테가노그래피 기법 이용

- **이미지(image) 스테가노그래피**
  - **팔레트 이미지**
    - ✓ 팔레트 : 0~255 사이의 정수 ➔ 256색을 나타냄
    - ✓ 하나의 픽셀은 팔레트 내의 하나의 색(color)을 나타내는 인덱스와 매칭됨



3. 스테가노그래피 기법 이용

- **이미지(image) 스테가노그래피**
  - **JPEG 압축 이미지 변환 과정**
    1. 컬러 변환(옵션) : RGB 모델에서 YIQ 모델로 변환
    2. YIQ의 매크로 블록(Macroblock)화
    3. 매크로 블록화를 8 * 8 블록화
    4. 이산 코사인 변환, DCT(Discrete Cosine Transform)
    5. 양자화(Quantization)
    6. 지그재그 스캐닝(Zig-zag Scanning)
    7. 엔트로피 코딩(Entropy Coding)

3. 스테가노그래피 기법 이용

▪ 이미지(image) 스테가노그래피

• 데이터 삽입(data insertion) 기법

✓ 대치 기법(Substitution systems) : 잉여 정보에 데이터 대치

- 순차 삽입(Serial embedding)
- 임의 삽입(Random embedding)

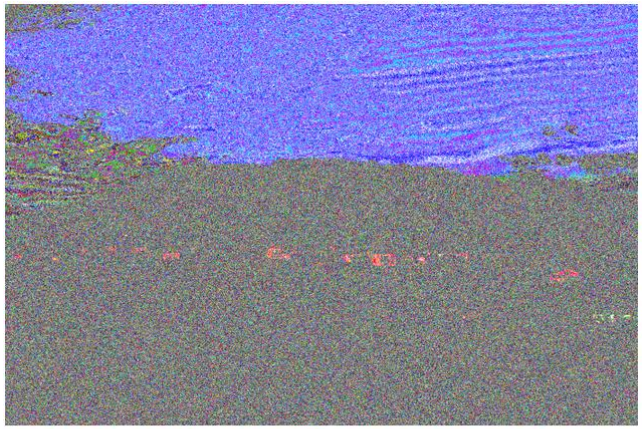
✓ 변환 영역 기법(Transform domain technique)

- JPEG DCT 영역에 데이터 삽입

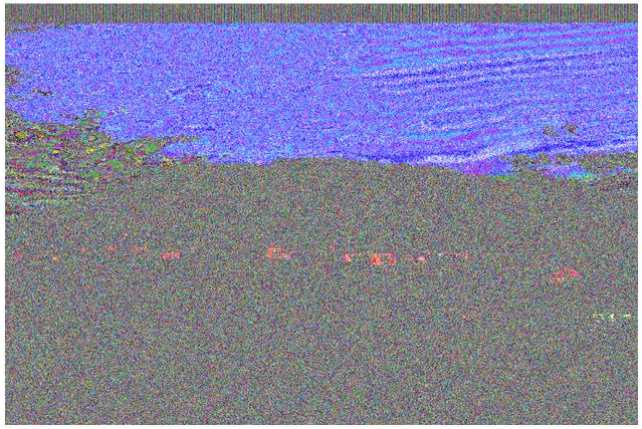
3. 스테가노그래피 기법 이용

- **이미지(image) 스테가노그래피**
  - **데이터 삽입(data insertion) ➔ 대치 기법**
    - ✓ LSB(Least Significant Bit) Embedding – 최하위 비트 대치

원본 이미지



LSB 기법에 의해 텍스트 은닉

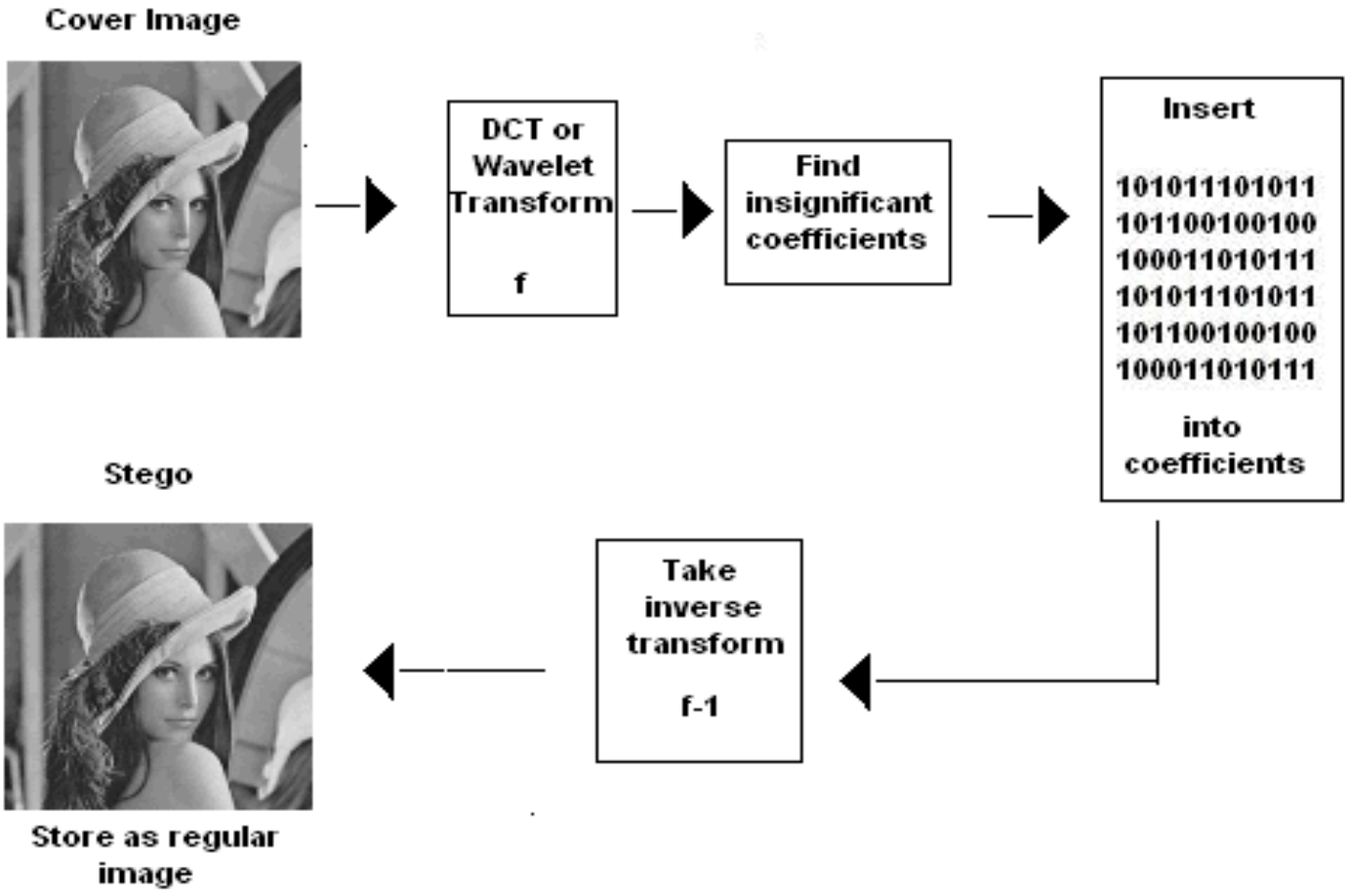


3. 스테가노그래피 기법 이용

- **이미지(image) 스테가노그래피**
  - **데이터 삽입(data insertion) ➔ 변환 영역 기법**
    - ✓ LSB 치환보다 안전한 방법
    - ✓ 신호처리 기술을 적용
    - ✓ 주파수 도메인(frequency domain)에 정보를 삽입하는 것이 시간 도메인(time domain)에 삽입하는 것보다 데이터 변경에 강인
    - ✓ 변환 영역 기법은 이미지의 중요 부분에 데이터를 삽입하는 방법
    - ✓ 변환 영역 예)
      - DCT(Discrete Cosine Transformation)
      - DFT (Discrete Fourier Transform)
      - Wavelet Transform
      - … …

3. 스테가노그래피 기법 이용

- 이미지(image) 스테가노그래피
  - 데이터 삽입(data insertion) ➔ 변환 영역 기법



3. 스테가노그래피 기법 이용

- **이미지(image) 스테가노그래피 ➔ 대응**
  - **시각 공격(Visual Attack)**
    - ✓ 잠재적인 메시지 비트를 필터링하거나 시각화
    - ✓ 빠르고, 간단히, 독립적으로 적용 가능
    - ✓ 기계적으로 판단하기는 어려움 ➔ 사람이 판단

Cover image

LSB plain of
the green channel
of the **cover image**

LSB plain of
the green channel
of the **stego image**


LSB plain of
the **stego image**

3. 스테가노그래피 기법 이용

▪ 오디오(Audio) 스테가노그래피

- **오디오 파일 포맷**

✓ 비압축 오디오 포맷 : PCM(Pulse Code Modulation)

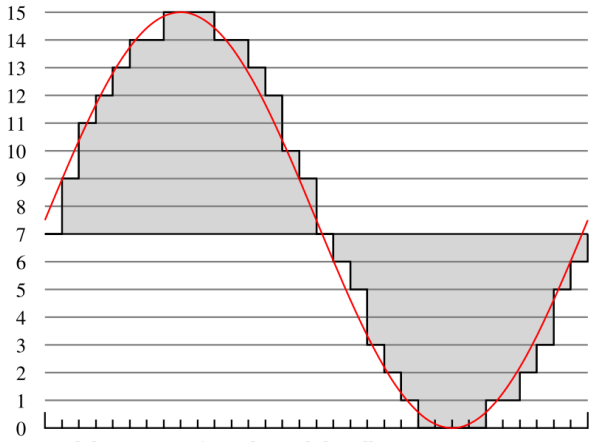
- 아날로그 시그널이 균등 분포
- WAV(Waveform Audio Format)

✓ 무손실 오디오 포맷

- TTA(True Audio Codec)
- FLAC(Free Lossless Audio Codec)

✓ 손실 오디오 포맷

- MP3 (MPEG-1 Audio Layer 3 Codec)
- WMA
- AAC



4-bit PCM of a signal (red)

3. 스테가노그래피 기법 이용

- 오디오(Audio) 스테가노그래피 기법
  - LSB Encoding
  - Echo Hiding
  - Phase Coding
  - Spread Spectrum

3. 스테가노그래피 기법 이용

- 스테가노그래피 도구
  - **S-Tools(Steganography Tools)** – http://bit599.netai.net/s_tools.htm
  - **Stego PNG –** http://www.hermetic.ch/stpng/stpng.htm
  - **OutGuess** – http://www.outguess.org/
  - **OmnHide** – http://omnihide.com/
  - **Our Secret** – http://www.securekit.net/
  - **Invisible Secret** – http://www.invisiblesecrets.com/steganography-software.html
  - **StegoMagic** – http://www.programmersheaven.com/download/38361/Download.aspx
  - **MP3Stego -** http://www.petitcolas.net/fabien/steganography/mp3stego/
  - **Mp3stegz –** http://sourceforge.net/projects/mp3stegz/
  - **CryptArkan –** http://www.kuskov.com/cryptarkan/
  - **Data Stash –** http://www.skyjuicesoftware.com/software/ds_info.html
  - **SlientEye –** http://www.silenteye.org/

3. 스테가노그래피 기법 이용

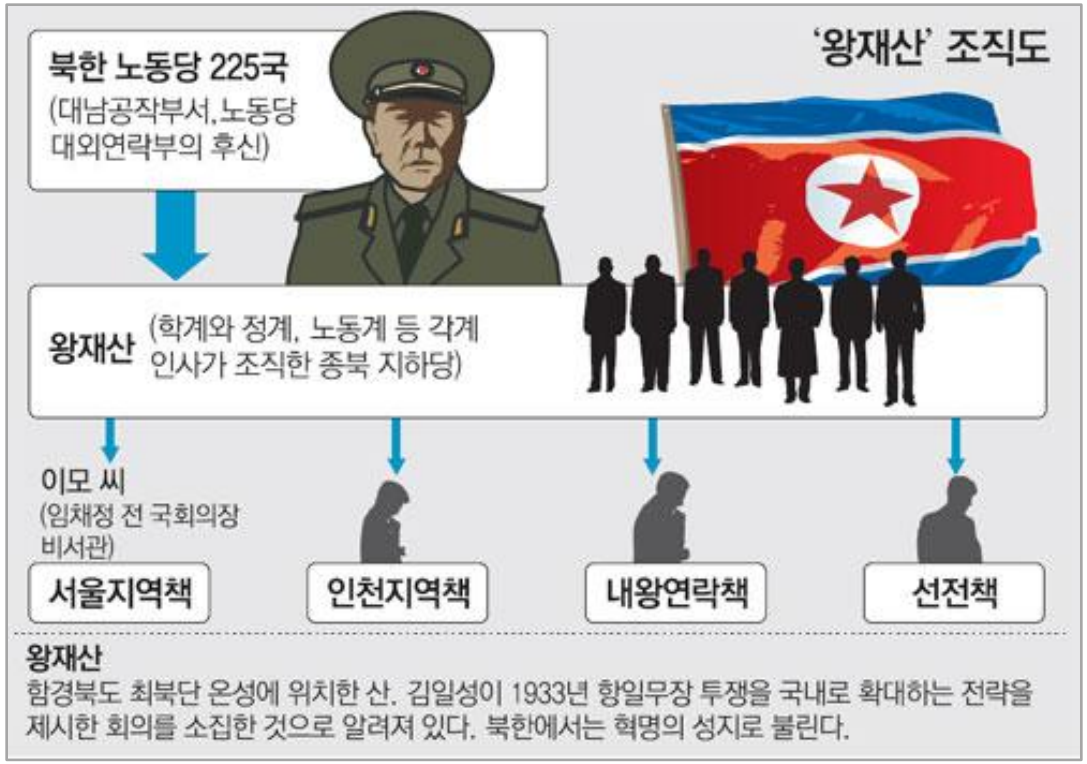
- # 실습 – 스테가노그래피 적용하기!!

1. 이미지 파일에 스테가노그래피 적용하기

2. 오디오 파일에 스테가노그래피 적용하기

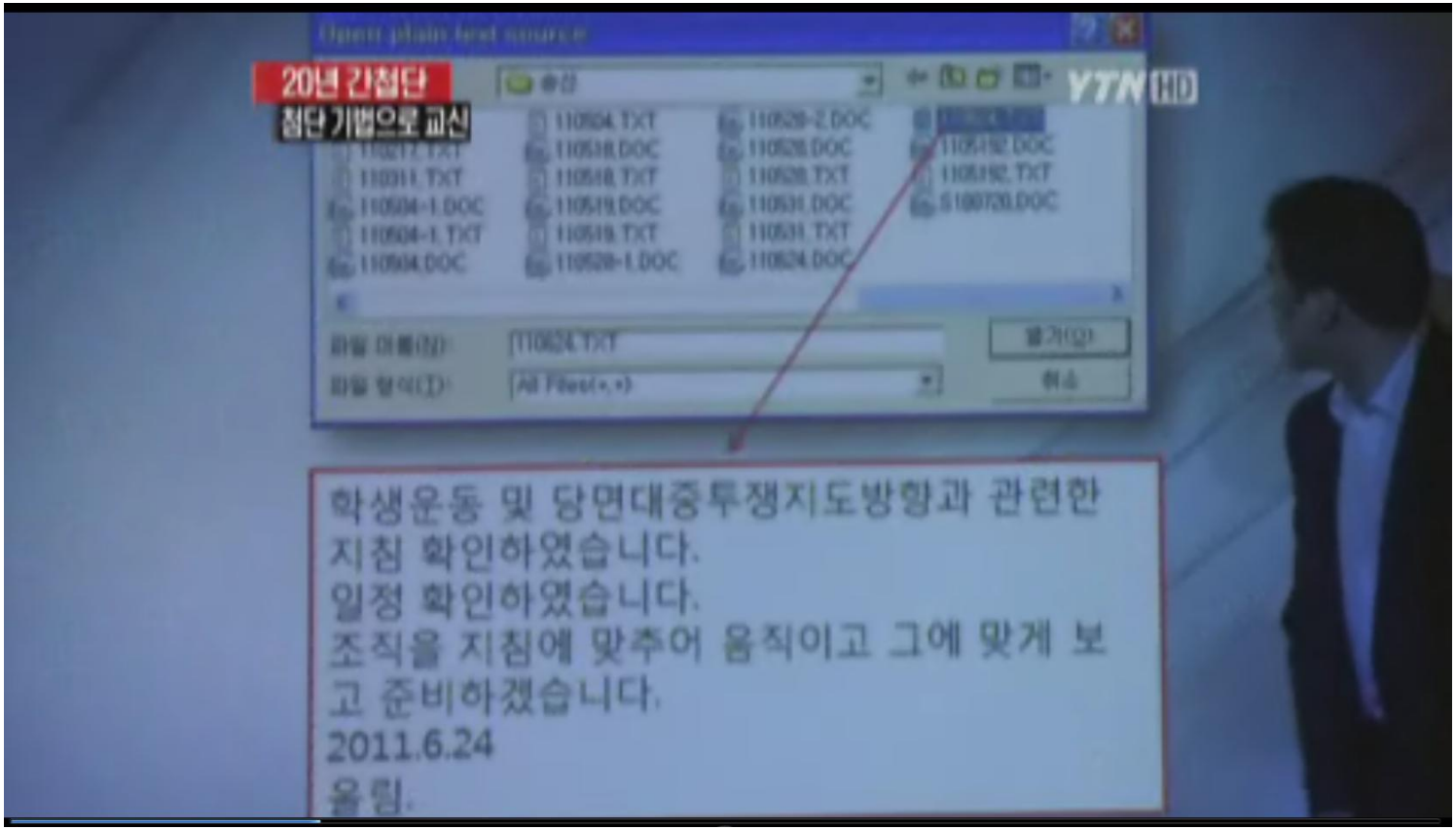
3. 스테가노그래피 기법 이용

- **사례 1 – 왕재산 간첩 사건 (2011.08)**
  - 김일성 직접 지령 ➔ 1993년 "남조선혁명을 위한 지역지도부를 구축하라"
  - 2001년 3월 왕재산 결성
  - 지난 10년간 활동



3. 스테가노그래피 기법 이용

- **사례 1 – 왕재산 간첩 사건 (2011.08)**
  - 비밀통신을 위해 스테가노그래피 기법 사용
  - 지령문, 대북보고문(Text)을 MS 워드 파일에 은닉하여 해외 이메일로 주고 받음



3. 스테가노그래피 기법 이용

▪ 사례 1 – 왕재산 간첩 사건 (2011.08)

- 왕재산 스테가노그래피 적용 과정 (서울중앙지검 제공)

1. 'CDSpace5.0Full' 폴더의 'data.hdr' 파일을 'data.exe'로, 'setup.bmp' 파일을 'set.bmp' 로 각각 변경
2. 'Recycled' 하위 폴더인 'data..'폴더의 'upgrade.exe' 파일을 실행하여 텍스트(txt) 파일 암/복호화 수행
3. 암호화된 txt 파일을 Microsoft 워드 파일에 은닉(hiding)하여 전송
4. 스테가노그래피 해독을 위해서 동일한 프로그램 사용

27) 예컨대, 2011. 6. 24. 작성 대북보고문 파일 '110624.txt'(학생운동 및 당면 대중투쟁지도방향과 관련한 지침을 확인하였다는 내용)을 변신프로그램으로 암호화하여 위장용 파일 '110624.doc'(31KB, '유럽을 죽음의 공포로 몰고간 슈퍼박테리아 정체 드러나' 제하 뉴스 기사)로 은닉한 후 '27s110624.doc'란 다른 이름으로 저장하여 위 '27s110624.doc' 파일을 실행하면 '110624.doc'에 저장된 뉴스 기사만 화면에 나타나고 대북보고문(110624.txt)은 나타나지 않는 것과 같은 방법이다.

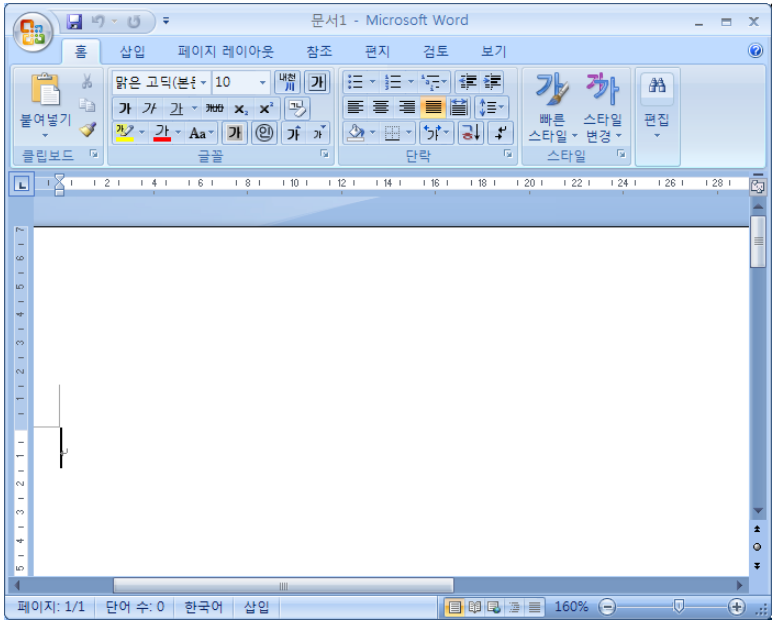
< 왕재산 1심 판결문 144쪽 내용 일부, 서울중앙지방법원>

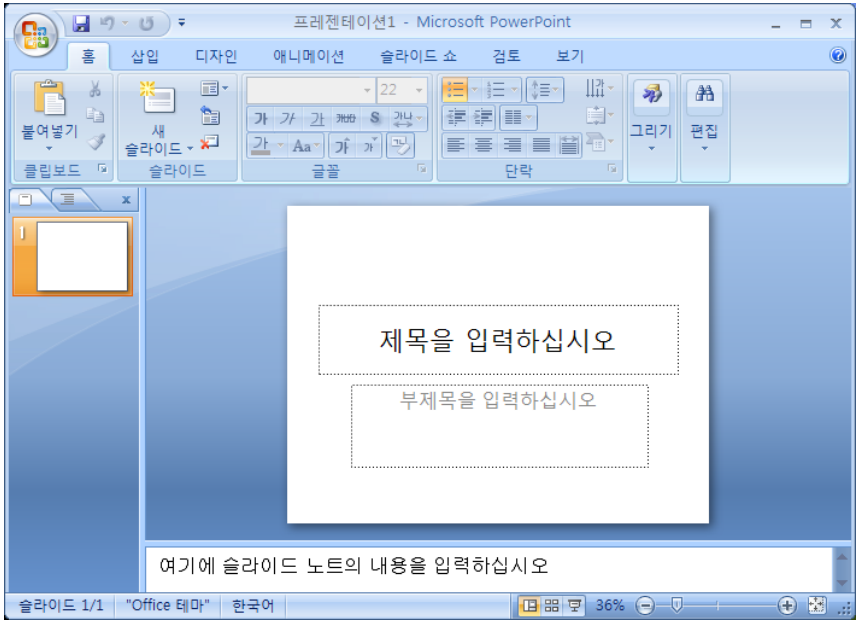
3. 스테가노그래피 기법 이용

▪ 문서 파일 스테가노그래피 기법

- **MS 오피스(워드/엑셀/파워포인트) 1997~2003 파일**

  ✓ 복합 파일 이진 형식(Compound File Binary Format)

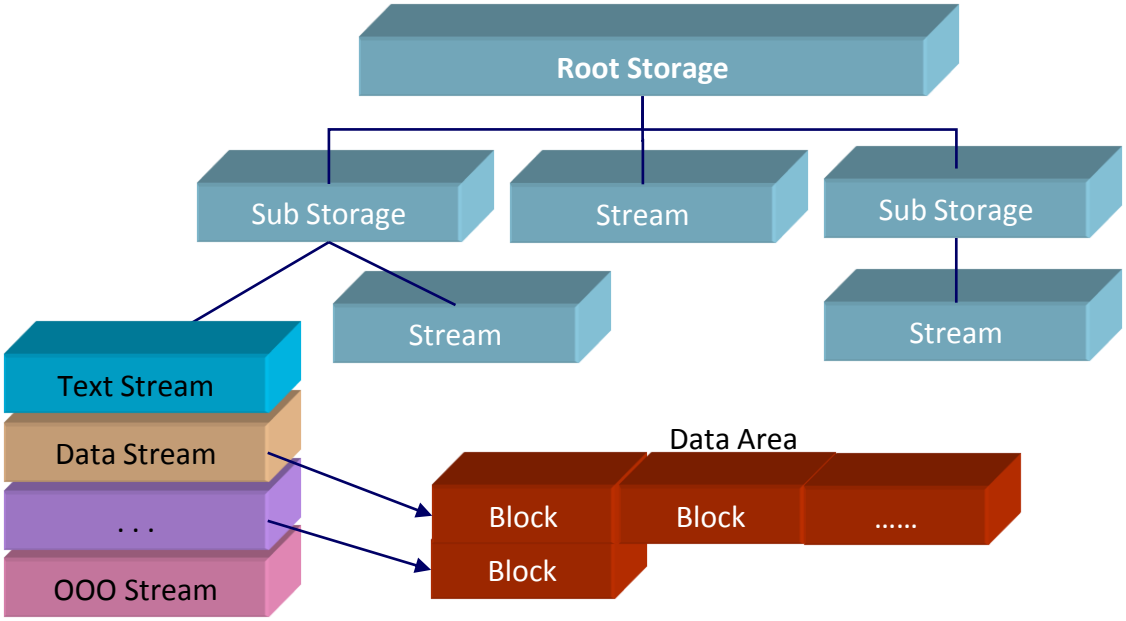




3. 스테가노그래피 기법 이용

▪ 문서 파일 스테가노그래피 기법

- **복합 파일 이진 형식(Compound File Binary Format)**
  - ✓ 파일시스템 FAT과 유사함
  - ✓ 스토리지(Storage)와 스트림(Stream)의 계층 구조로 구성
  - ✓ 비할당, 슬랙 영역을 이용하여 "데이터 은닉" 가능



3. 스테가노그래피 기법 이용

▪ 문서 파일 스테가노그래피 기법

• 복합 파일 이진 형식(Compound File Binary Format)

✓ 비할당 & 슬랙 영역

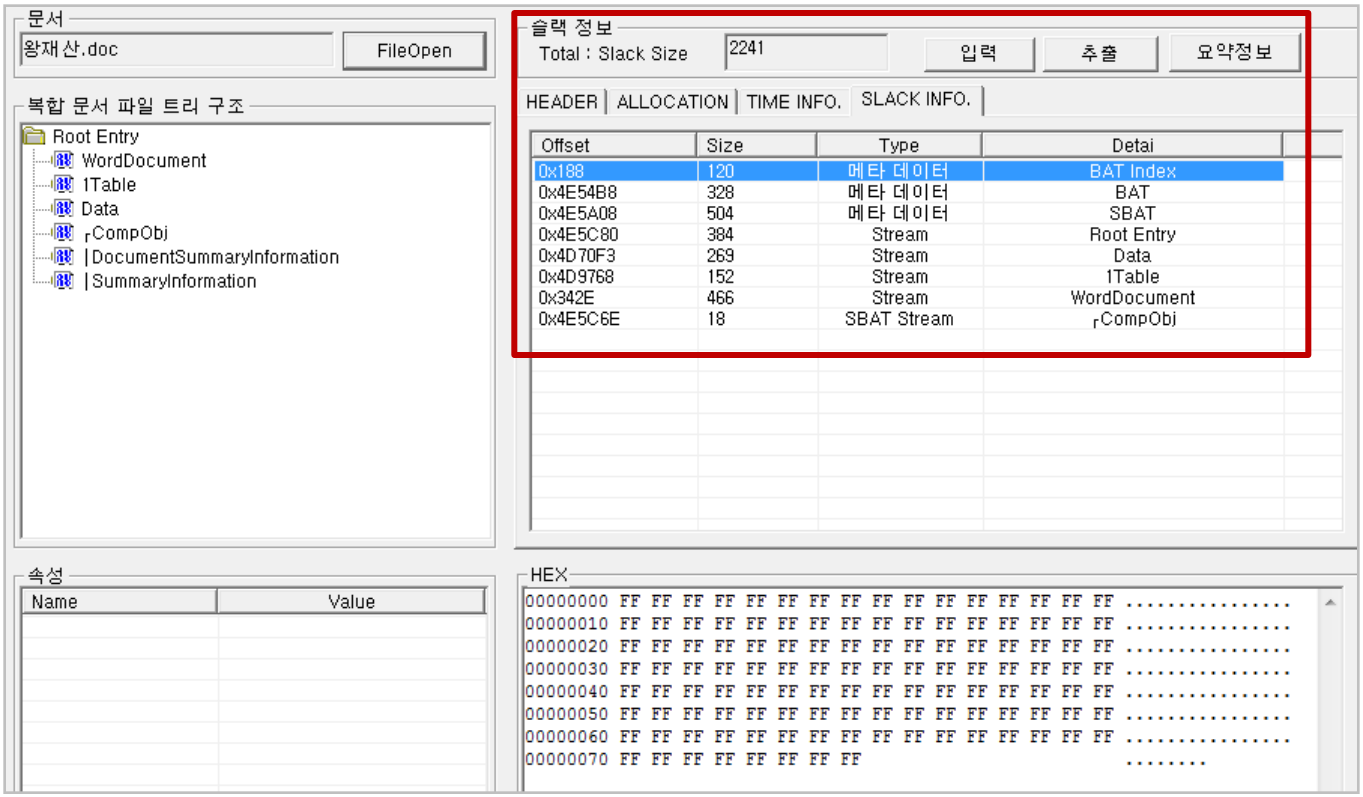
- 블록 단위로 데이터를 할당하기 때문에 파일시스템처럼 비할당과 슬랙 영역이 존재

3. 스테가노그래피 기법 이용

▪ 문서 파일 스테가노그래피 기법

• 복합 파일 이진 형식(Compound File Binary Format)

✓ 비할당 & 슬랙 영역에 데이터 은닉



< MS 워드 파일 내의 비할당 & 슬랙 영역 확인 >

3. 스테가노그래피 기법 이용

▪ 문서 파일 스테가노그래피 기법

- **복합 파일 이진 형식(Compound File Binary Format)**

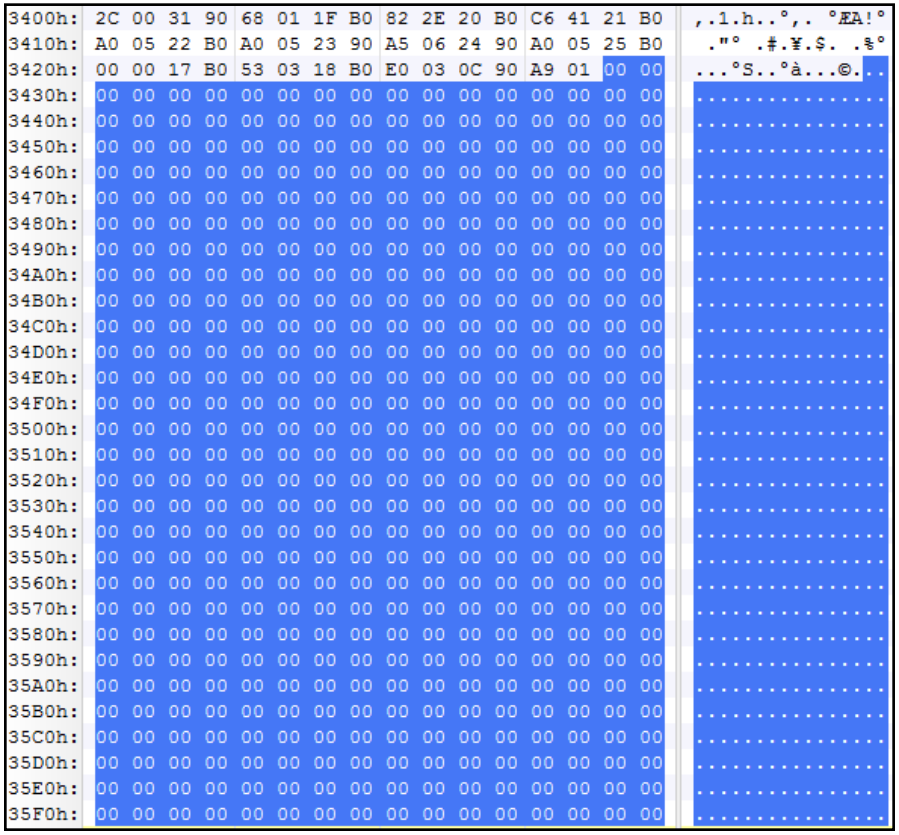
  ✓ 비할당 & 슬랙 영역에 데이터 은닉

학생운동 및 당면대중투쟁지도방향과 관련한
지침 확인하였습니다.
일정 확인하였습니다.
조직을 지침에 맞추어 움직이고 그에 맞게 보고
준비하겠습니다.
2011.6.25
올림.

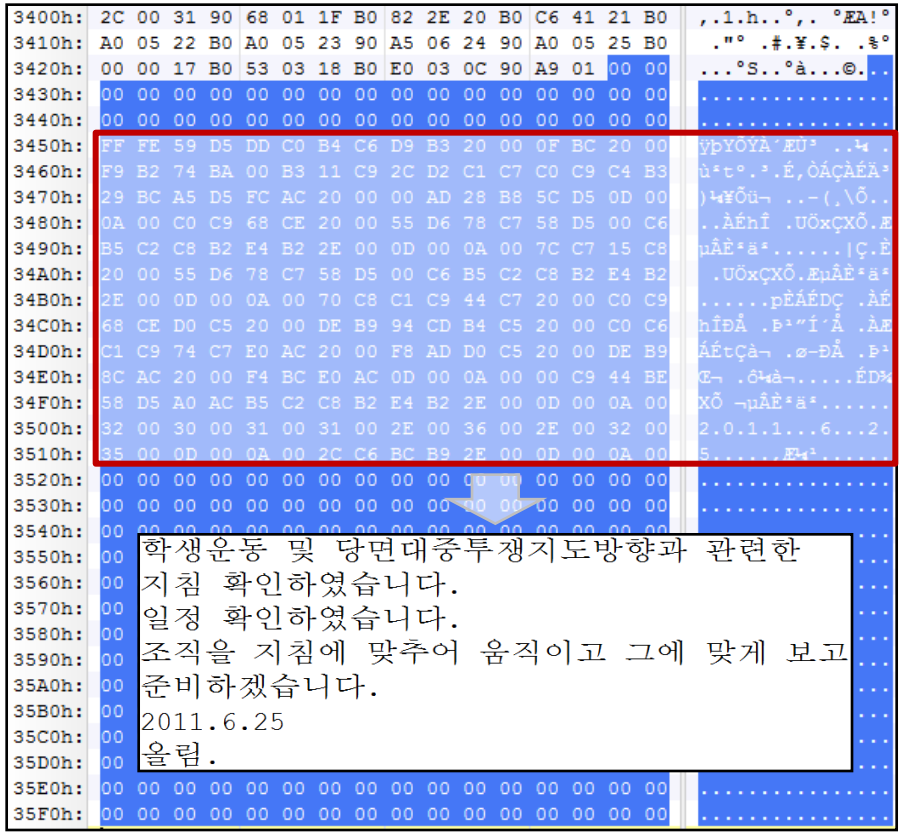
< 은닉할 비밀 메시지 (secret message.txt) >

3. 스테가노그래피 기법 이용

- **문서 파일 스테가노그래피 기법**
  - **복합 파일 이진 형식(Compound File Binary Format)**
    - ✓ 비할당 & 슬랙 영역에 데이터 은닉



< 비밀 메시지 은닉 전 : 사용되지 않는 비할당 영역 >



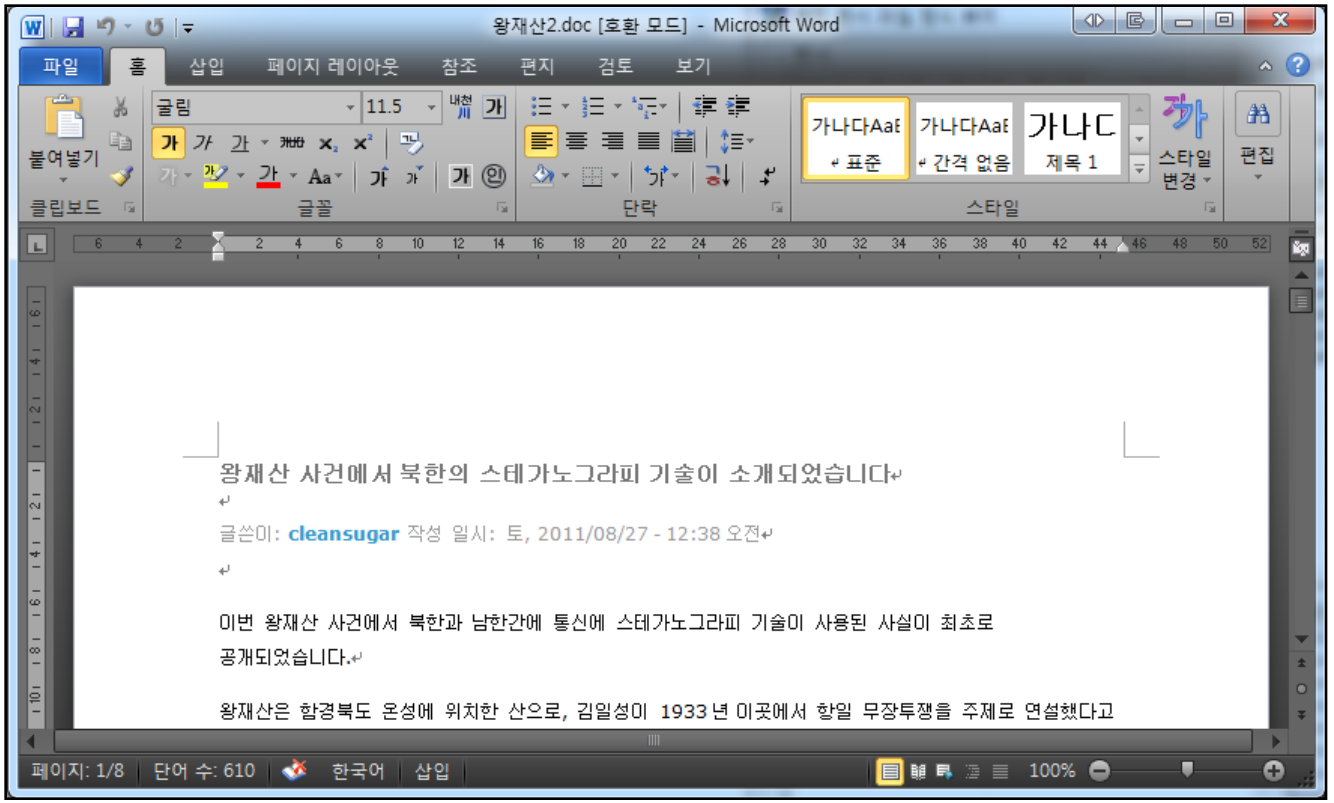
< 비밀 메시지 은닉 후 : 사용되지 않는 비할당 영역 >

3. 스테가노그래피 기법 이용

▪ 문서 파일 스테가노그래피 기법

• 복합 파일 이진 형식(Compound File Binary Format)

✓ 비할당 & 슬랙 영역에 데이터 은닉

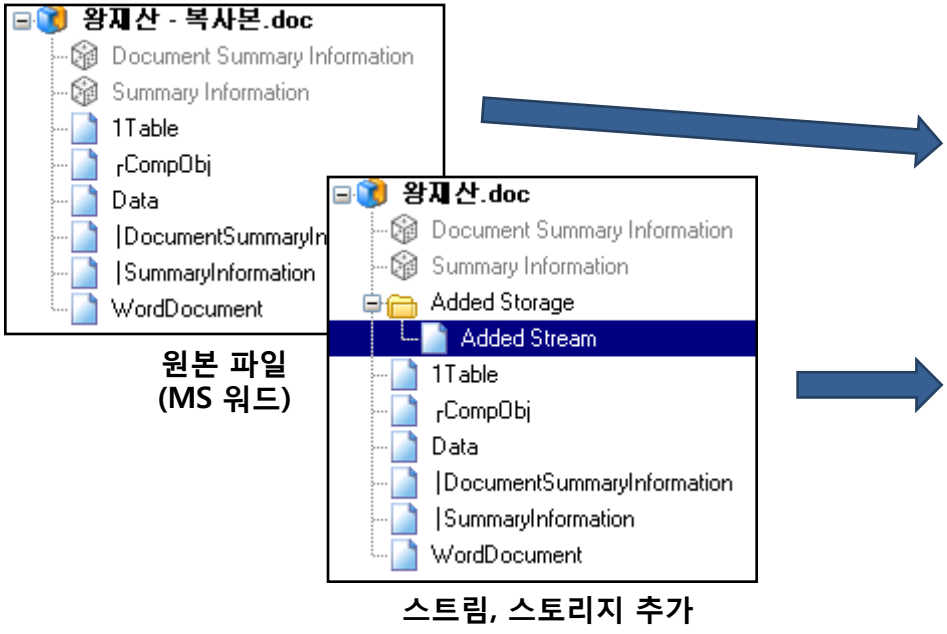


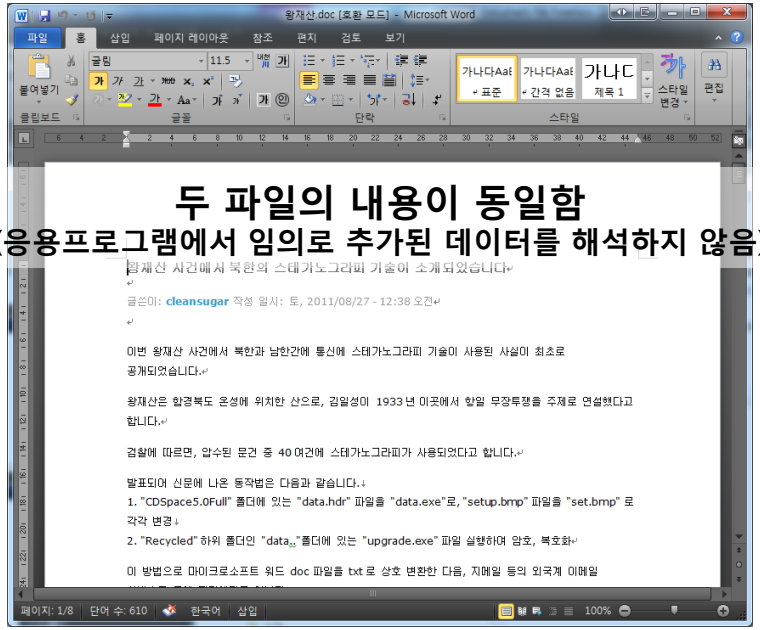
< 비밀 메시지 은닉 후, 파일 내용 확인 : '비밀 메시지는 확인할 수 없음' >

3. 스테가노그래피 기법 이용

▪ 문서 파일 스테가노그래피 기법

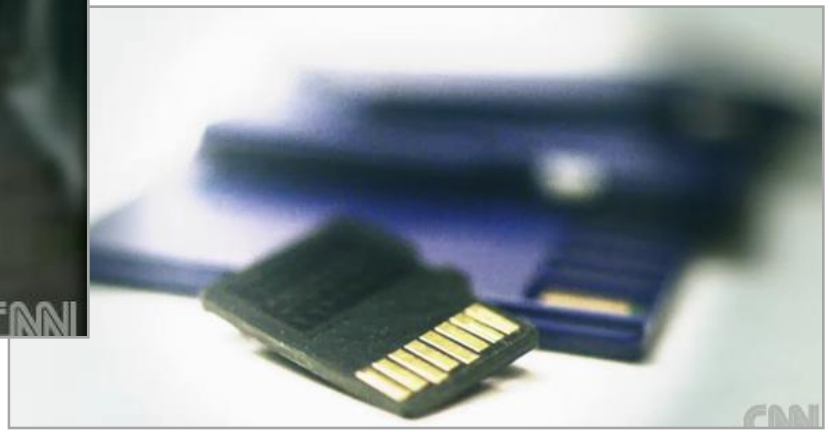
- **복합 파일 이진 형식(Compound File Binary Format)**
  - ✓ 직접 스트림, 스토리지를 추가하여 데이터 은닉
    - 추가 #1 : 윈도우 API를 직접 호출하여 구현
    - 추가 #2 : SSView, CFX 등의 복합문서 분석 도구를 사용
    - 추가된 스트림, 스토리지는 응용프로그램에서 인식하지 않음





3. 스테가노그래피 기법 이용

- **사례 2 – 알 카에다 비밀문서 (2012.05)**
  - 비디오 스테가노그래피 사례
  - 오스트리아 국적의 "맥수드 로딘(22)"은 독일 베를린에서 체포됨
  - 속옷에서 "메모리 카드" 발견



3. 스테가노그래피 기법 이용

- **사례 2 – 알 카에다 비밀문서 (2012.05)**
  - 다수의 포르노 영상 발견 – 엉덩이를 차라(kick ass), 섹시한 탄자(sexy tanja) 등
  - 독일 수사 당국의 포르노 분석 결과 ➔ 100건이 넘는 알카에다 비밀 문서 발견
  - 비밀 문서 : 미래의 작전(future works)
    - ✓ 과거의 테러 기록 : 2008년 인도 뭄바이 테러 등
    - ✓ 향후 테러 계획 포함
    - ✓ 테러리스트 교육 자료 포함(독일어, 영어, 아랍어 등) ➔ PDF

데이터 조작 기법

데이터 조작 기법

1. 파일 속성 조작

1. 파일 속성 조작

▪ 파일 속성 조작?

- 파일의 메타데이터를 변경하여 분석을 방해하는 행위

- **파일시스템 메타데이터 변조**
  - ✓ 파일 이름, 파일 시간정보, 파일 특성 등

- **파일 헤더 변조**
  - ✓ 파일 헤더의 메타데이터 변조

- **대응**
  - ✓ 파일시스템의 모든 시간(8개)을 정렬, 분석하여 의심 파일 탐지
  - ✓ 통합 타임라인 분석을 통해 비정상적인
  - ✓ 파일 속성 조작 도구의 설치 혹은 실행 흔적 탐지

1. 파일 속성 조작

- **파일 속성 조작 도구**
  - **setMACE** – http://reboot.pro/files/file/91-setmace/
  - **Timestomp** – http://www.offensive-security.com/metasploit-unleashed/Timestomp
  - **eXpress TimeStamp Toucher (XTST)** – http://www.irnis.net/soft/xtst/
  - **Moo0 Window Menu Plus** – http://kor.moo0.com/software/WindowMenuPlus/
  - **Moo0 Time Stamp** – http://kor.moo0.com/software/TimeStamp/
  - **Moo0 Mp3 Info Editor** – http://kor.moo0.com/?top=http://kor.moo0.com/software/Mp3InfoEditor/
  - **Attribute Changer** – http://www.petges.lu/home/download/
  - **BulkFileChanger** – http://www.nirsoft.net/utils/bulk_file_changer.html

1. 파일 속성 조작

▪ 파일 시간 조작

- 자신을 은닉하기 위해 시스템 주요 파일(ntdll.dll, rundll32.exe 등)과 시간 동기화

- **SetFileTime() API (Kernel32.dll)**
  - ✓ 생성, 수정, 접근 시간만 수정 가능
  - ✓ MFT 레코드 수정 시간을 이용해 쉽게 탐지 가능

- **NtSetInformationFile() API (NTDLL.dll)**
  - ✓ 생성, 수정, 접근, MFT 레코드 수정 시간 모두 변경 가능
  - ✓ $FILE_NAME 속성을 이용해 탐지 가능

1. 파일 속성 조작

▪ 파일 시간 탐지

- 생성 시간, MFT 레코드 수정 시간 등을 정렬하여 시스템 설치 시간 대에 의심 파일 생성 확인

Drive C:

Windows\System32 — 21 days ago

Name	Ext.	Size	Created	Modified	Accessed	Record update	Attr.	1st sector
PSHED.DLL	DLL	56.1 KB	2009-07-14 08:19:28	2009-07-14 10:45:45	2009-07-14 08:19:28	2012-03-04 10:07:36	A	185792
clfsw32.dll	dll	77.5 KB	2009-07-14 08:19:34	2009-07-14 10:40:15	2009-07-14 08:19:34	2012-03-04 10:06:59	A	139017...
txfw32.dll	dll	11.5 KB	2009-07-14 08:19:38	2009-07-14 10:41:55	2009-07-14 08:19:38	2012-03-04 10:07:44	A	8168856
services.exe	exe	321 KB	2009-07-14 08:19:46	2009-07-14 10:39:37	2009-07-14 08:19:46	2012-03-04 10:07:39	A	226920
csrss.exe	exe	7.5 KB	2009-07-14 08:19:49	2009-07-14 10:39:02	2009-07-14 08:19:49	2012-03-04 10:07:00	A	119760
smss.exe	exe	110 KB	2009-07-14 08:19:50	2009-07-14 10:39:41	2009-07-14 08:19:50	2012-03-04 10:07:41	A	436696
clfs.sys	sys	359 KB	2009-07-14 08:19:59	2009-07-14 10:52:31	2009-07-14 08:19:59	2012-03-04 10:06:59	A	367256
api-ms-win-security-lsal...	dll	3.5 KB	2009-07-14 08:20:47	2009-07-14 10:24:53	2009-07-14 08:20:47	2012-03-04 10:06:55	HA	110636...
api-ms-win-security-sdd...	dll	3.0 KB	2009-07-14 08:20:47	2009-07-14 10:24:53	2009-07-14 08:20:47	2012-03-04 10:06:55	HA	110666...
sechost.dll	dll	111 KB	2009-07-14 08:20:52	2009-07-14 10:41:53	2009-07-14 08:20:52	2012-03-04 10:07:39	A	332464
cryptbase.dll	dll	43.0 KB	2009-07-14 08:20:54	2009-07-14 10:40:24	2009-07-14 08:20:54	2012-03-04 10:07:00	A	94720
profapi.dll	dll	43.0 KB	2009-07-14 08:20:57	2009-07-14 10:41:53	2009-07-14 08:20:57	2012-03-04 10:07:36	A	134208
netevent.dll	dll	18.5 KB	2009-07-14 08:20:58	2009-07-14 10:30:47	2009-07-14 08:20:58	2012-03-04 10:07:19	A	144538...
nsi.dll	dll	13.5 KB	2009-07-14 08:21:05	2009-07-14 10:41:53	2009-07-14 08:21:05	2012-03-04 10:07:33	A	103296
RpcEpMap.dll	dll	65.5 KB	2009-07-14 08:21:05	2009-07-14 10:41:53	2009-07-14 08:21:05	2012-03-04 10:07:37	A	133952
winnsi.dll	dll	25.5 KB	2009-07-14 08:21:08	2009-07-14 10:41:56	2009-07-14 08:21:08	2012-03-04 10:07:48	A	176744
dhcpcsvc6.dll	dll	53.0 KB	2009-07-14 08:21:09	2009-07-14 10:40:28	2009-07-14 08:21:09	2012-03-08 08:32:33	A	192704
dhcpcsvc.dll	dll	85.0 KB	2009-07-14 08:21:09	2009-07-14 10:40:28	2009-07-14 08:21:09	2012-03-08 08:32:33	A	151104
dhcpcore6.dll	dll	219 KB	2009-07-14 08:21:13	2009-07-14 10:40:28	2009-07-14 08:21:13	2012-03-08 08:32:33	A	447512
IPHLPAPI.DLL	DLL	143 KB	2009-07-14 08:21:13	2009-07-14 10:41:10	2009-07-14 08:21:13	2012-03-04 10:07:11	A	276512
dhcpcore.dll	dll	307 KB	2009-07-14 08:21:15	2009-07-14 10:40:28	2009-07-14 08:21:15	2012-03-04 10:07:02	A	446896
api-ms-win-core-ums-l1...	dll	3.0 KB	2009-07-14 08:21:15	2009-07-14 10:24:53	2009-07-14 08:21:15	2012-03-04 10:06:55	HA	110257...
shimeng.dll	dll	6.5 KB	2009-07-14 08:21:19	2009-07-14 10:41:54	2009-07-14 08:21:19	2012-03-08 08:32:37	A	8033728

1. 파일 속성 조작

- # 실습 – 파일 속성 조작 실습하기!!

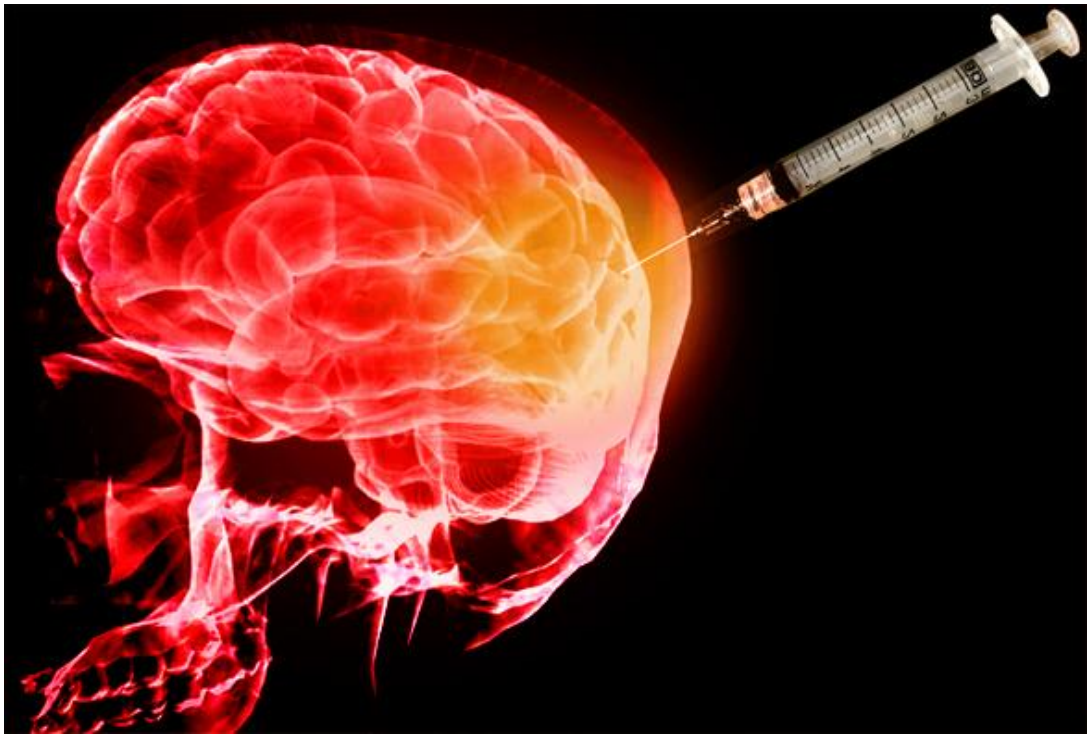
1. 시간 정보 조작 도구를 실행한 후 흔적 비교하기

2. 샘플 $MFT에서 시간 정보가 조작된 파일 분석하기

흔적 최소화 기법

흔적 최소화 기법

1. 포터블 프로그램 이용
2. 부터블 프로그램 이용
3. 가상 머신 이용
4. 메모리 인젝션 이용
5. 원격 코드 실행 이용



흔적 최소화 기법

1. 포터블 프로그램 이용

- **포터블 프로그램**
  - 프로그램을 시스템에 설치하지 않고 바로 실행할 수 있는 프로그램 형태
  - 설치 과정에서 남기는 아티팩트를 남기지 않음
  - 실행 과정에서 남기는 아티팩트 분석에 한정

- **대응**
  - ✓ **파일 생성 흔적 분석**
    - 파일시스템 로그 – $LogFile, $UsnJrnl
    - MFT, INDX 슬랙 분석
  - ✓ **폴더 열람 흔적 분석**
    - 레지스트리 셸백
  - ✓ **프로그램 실행 흔적 분석 고도화**
    - 프리패치 파일
    - 바로가기 파일
    - 점프 목록
    - … …

2. 부터블 프로그램 이용

- **부터블 프로그램**
  - 부팅이 가능한 형태로 시스템 운영체제를 동작시키지 않고 행위 ➔ 라이브 CD, 부팅 USB 등
  - 실행 과정의 아티팩트가 남지 않음
  - **대응**
    - ✓ **매체 제어 강화**
      - 매체 제어 솔루션 무력화
      - 보안 스티커나 별도의 방안 마련

3. 가상 머신 이용

- **가상 머신**
  - 시스템 운영체제 상에서 혹은 병행하여 추가적인 운영체제 구동 가능
  - 행위를 한 후 가상 머신 파일만 완전 삭제
  - **대응**
    - ✓ **가상 머신 아티팩트 분석만 가능**
      - 가상 머신 설치 및 사용 패턴, 시간 정보 등

4. 메모리 인젝션 이용

- **메모리 인젝션**
  - 일부 악성코드의 경우 익스플로잇 후 추가 파일 다운로드 없이 바로 메모리에서 삽입되어 행위
  - **대응**
    - ✓ **신속한 라이브 대응 중요**
      - 메모리 덤프 후 분석
      - 패킷 덤프 후 분석

5. 원격 코드 실행 이용

- **원격 코드 실행**
  - 프로세스가 익스플로잇되어 원격에 위치한 임의 코드 실행이 가능한 경우
  - 원격 코드를 전송받아 메모리 인젝션 후 실행

  - **대응**
    - ✓ **신속한 라이브 대응 중요**
      - 메모리 덤프 후 분석
      - 패킷 덤프 후 분석

질문 및 답변