2021 Winter wheel seminar #+: Antiforensic

2021.1.22. ivy

Contents

Antiforensic?

- Antiforensic
  - 민감한 데이터가 복구될 수 없도록 완전히 폐기하는 것
  - forensic
    - 삭제된 데이터를 복구해 내는 것
    - (英) '범죄 수사의', '법의학의'

~/Introduction/ >

Reality of deletion

취재진이 무작위로 중고 하드디스크 25개를 구입한 뒤, 간단한 복원 프로그램을 이용해 데이터가 있는지 없는지 확인해 봤습니다.

그 결과 20개 하드디스크에서 255만 9천 개의 파일을 복구했습니다.

주민등록증과 개인 통장 사본, 휴대전화 번호가 적힌 주소록은 물론 기업체의 세금계산서와 견적서까지,

민감한 개인정보와 기업 정보들이 마구 쏟아집니다.

<인터뷰>이상진(고려대 교수): "포맷을 하면 파일의 목록 정도가 없어지는 거고 실제 파일의 콘텐츠는 지워지지 않습니다."

HDD forensic

- HDD
  - 자기장을 이용해 데이터 저장
  - 데이터를 덮어써도…
    - 기존 데이터가 미세한 자기장의 형태로 잔류

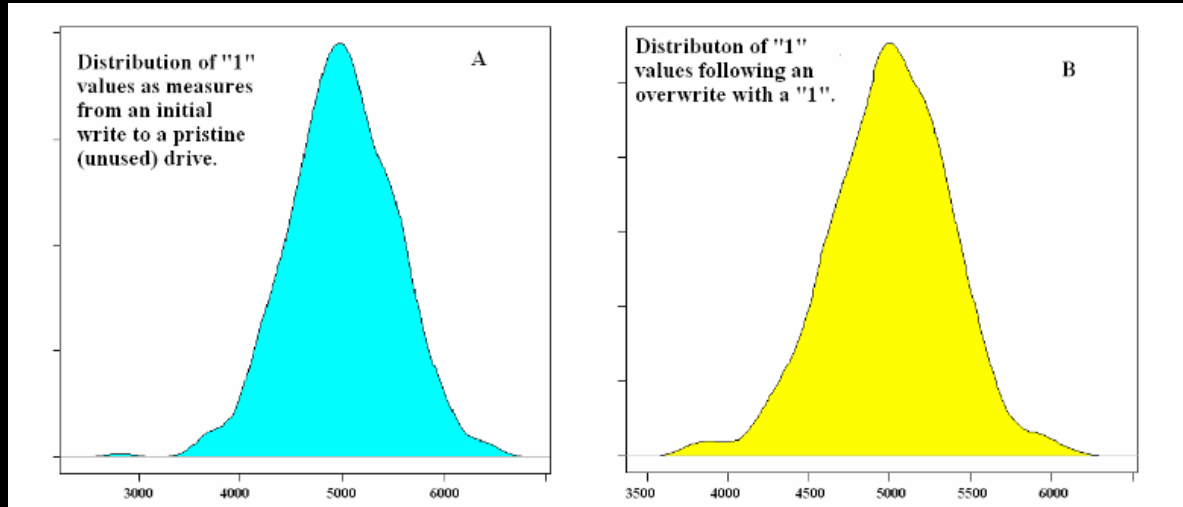
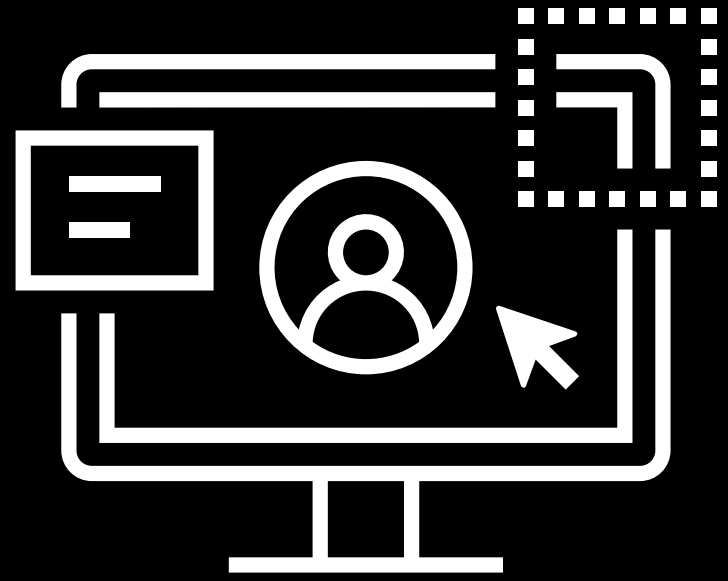


Fig. 5. This example displays the experimentally derived magnetic field density functions for hard drive rewrites where "A" displays the measured distribution of binary "1" values on initial copy. "B" displays the distribution of values associated with a binary "1" value following an overwrite with another binary "1".

[1] Wright, C., Kleiman, D., & Sundhar R.S., S. (2008). *Overwriting Hard Drive Data: The Great Wiping Controversy. Lecture Notes in Computer Science, 243–257.* doi:10.1007/978-3-540-89862-7_21

Data elimination

- Data elimination
  - HDD의 잔류 자기 등 복구 가능성이 있는 데이터를 파괴하는 것
    - 개인정보 보호
    - 민감한 데이터 폐기
    - 저장 장치 재사용 및 중고 판매
  - 주로 존재하는 데이터를 여러 번 덮어쓰는 방식으로 작동함
    - wiping, '소거'



Wiping standards

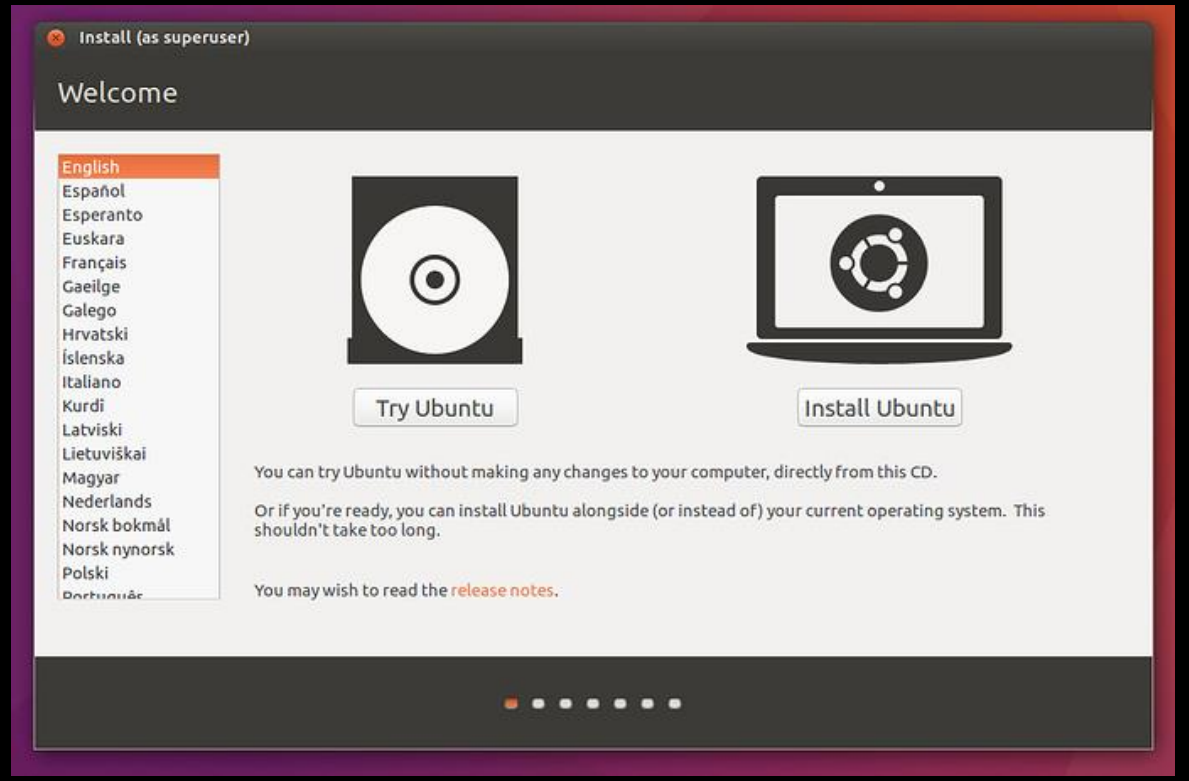
- Wiping standards
  - US DoD 5220.22-M
    - (2006). 미 국방부 보안 매뉴얼. 다양한 소거 방법이 있음
    - 주로 3-pass, 혹은 7-pass
  - Peter Gutmann's Algorithm
    - (1996). 무려 35번씩 덮어쓰는 알고리즘
    - 과거의 저장장치들을 소거하기 위해 고안됨. 35-pass
  - NIST SP-800-88 Rev. 1
    - (2014). 미 국립표준기술연구소 "미디어 소거 가이드라인"
    - 각 저장장치 종류에 따른 적절한 소거 방법이 제시됨 (HDD의 경우 1회 zero-fill로 충분)

US DoD 5220.22-M

- US DoD 5220.22-M
  - 2006년 미 국방부에서 제시한 소거 방법 표준. 가장 흔하게 쓰임
    - 국방부 문서 자체에는 소거 방법이 드러나 있지 않고, 구체적인 방법은 '타 기관의 문서를 참고'하라고만 되어 있음. 알려진 방법은 다음과 같음
  - US DoD 5220.22-M(8-306./E)
    - 3-pass. 데이터를 세 번 덮어씀. 'DoD short'
      - 일반적인 구현: zero-fill, one-fill, random-fill, verify
  - US DoD 5220.22-M(8-306./ECE)
    - 7-pass. 데이터를 일곱 번 덮어씀.
      - 3-pass를 하고, 특정 문자 데이터로 덮어쓰고, 3-pass를 함

Linux commands

- Linux commands
  - 데이터 소거에 사용할 수 있는 다양한 명령어 존재
    - dd, shred, blkdiscard, diskpart, …
  - Ubuntu Live USB로 부팅 후 이용하면 편리함



DBAN

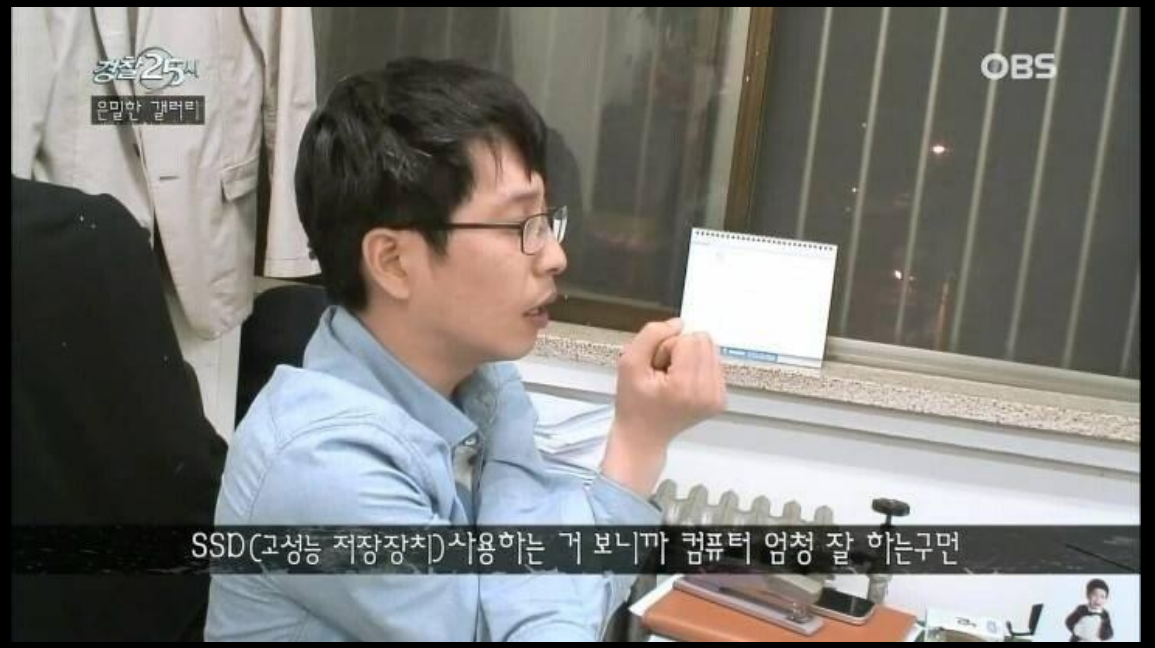
- DBAN
  - Darik's Boot And Nuke
    - 데이터 소거를 할 수 있는 부팅 디스크
      - USB에 iso를 구워서 사용
    - 장치 단위의 소거만 가능
      - ex) `/dev/sda`
    - 다양한 소거 방법 지원
      - DoD short, 7-pass, Gutmann, PRNG, …
    - 새파란 화면 (무서움)
      - 엘모는 없음

Encryption

- Encryption
  - 애초에 소거할 필요가 없도록 데이터를 암호화해서 저장
    - Bitlocker
      - Windows에서 사용할 수 있는 파티션 암호화 프로그램
      - Windows Pro 이상에서만 사용 가능
    - Veracrypt
      - Truecrypt의 fork. 리눅스, 맥, 윈도우 지원. 파티션 암호화, 암호화 볼륨 만들기 등 지원
      - 다양한 암호화 알고리즘 지원. 보안성 매우 높음. 느림
  - 데이터가 필요없어지면 암호화 키를 폐기
    - 키가 없는 암호문은 해독 불가한 쓰레기 데이터

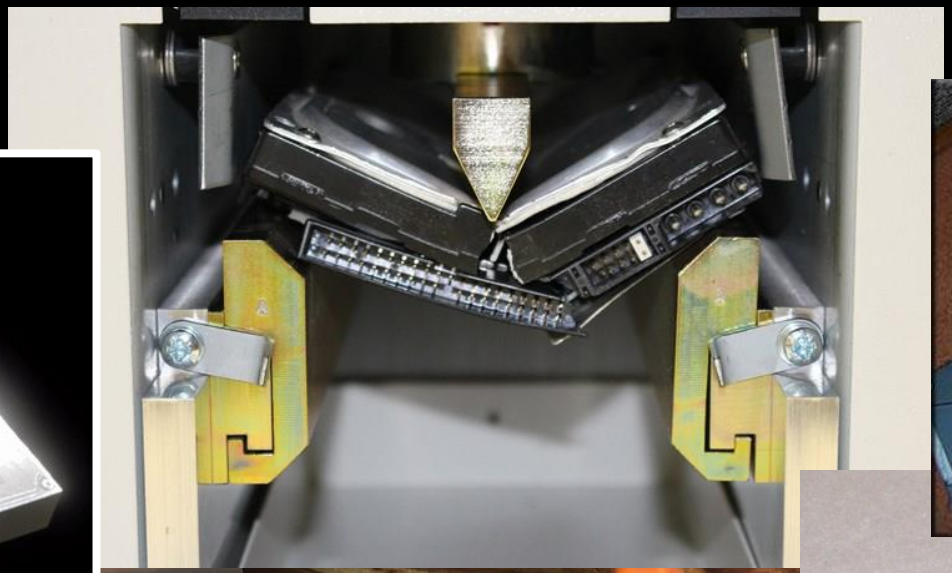
SSD

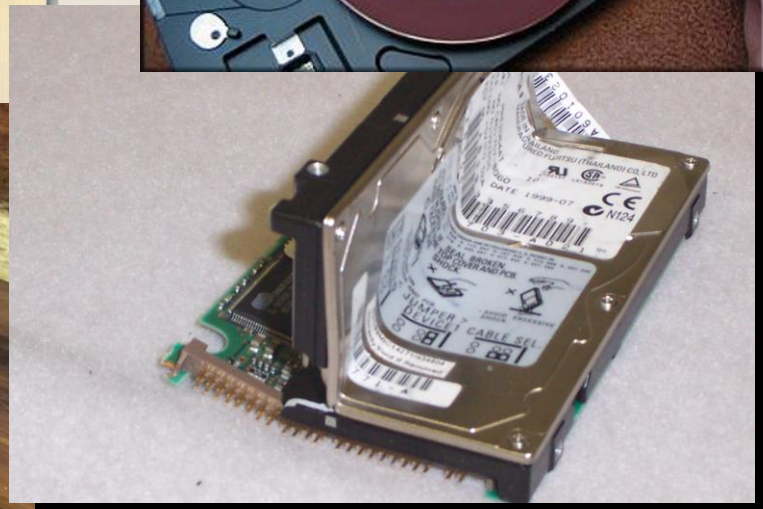
- SSD
  - 자체 최적화로 인해 HDD의 소거 방식은 통하지 않음
    - SSD의 데이터 셀은 쓰면 쓸수록 수명이 줄어듬
    - HDD의 '덮어쓰기'가 먹히지 않음
      - 쓰기 명령 시 쓰는 위치를 SSD가 자의적으로(!) 판단함
    - TRIM: 데이터 삭제 명령 시 SSD가 알아서 판단해서 적절한 때에 데이터 셀을 실제로 초기화
    - ∴ 소거를 위해서는 특수한 툴 사용
      - 제조사 제공 프로그램



~/Methods/ >

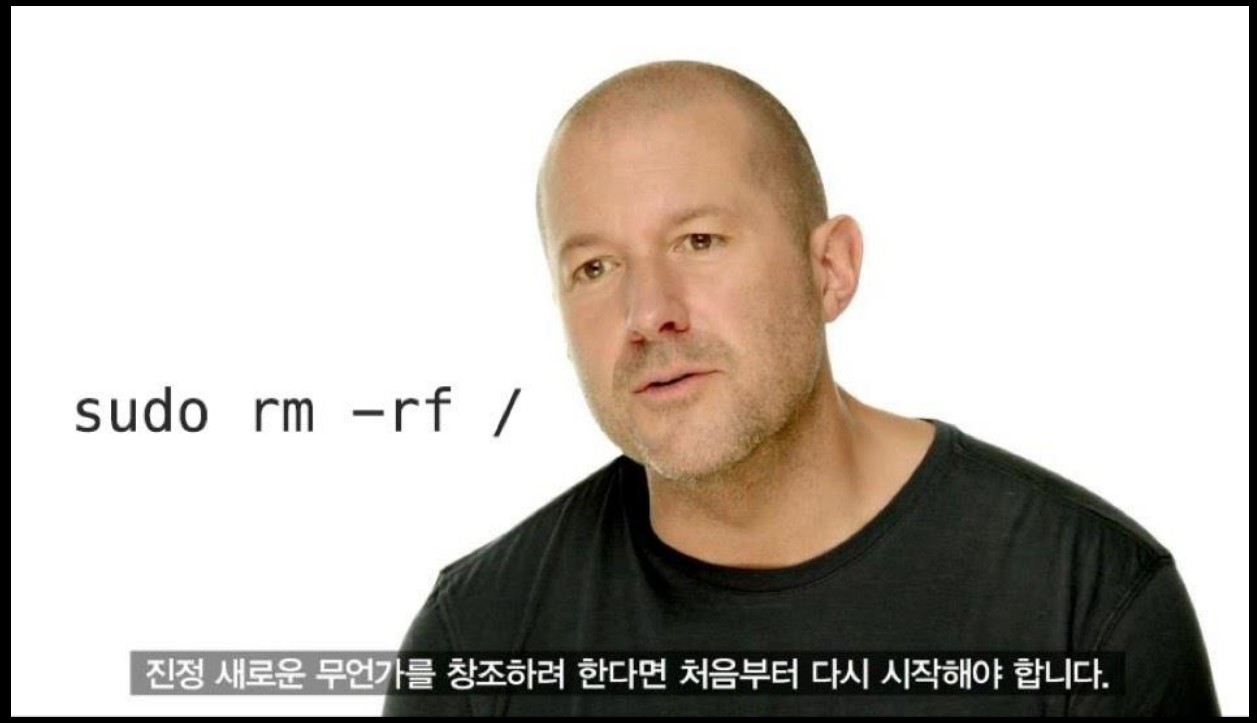
Physical methods





rm -rf (?)

- rm -rf
  - rm 명령어는 파일 내용은 지우지 않음
    - inode만 삭제(되었다고 표기)
    - 실제로 데이터가 소거되지 않음
    - 소거 목적으로 사용할 수 없음



dd

- dd
  - 파일 복사 및 변환 명령어
    - 원래는 서로 다른 인코딩 사이의 변환을 위한 유틸리티로 출발함
  - `dd if=/dev/urandom of=/dev/sdb3 bs=4096 status=progress`
    - 의사난수 스트림(/dev/urandom)에서 4KiB씩 읽어서 소거 대상 장치에 쓰는 명령어
    - 대상 장치(/dev/sdb3)의 각 섹터가 소거됨
    - status=progress 옵션: 진행 상황을 보여줌 (소거된 용량, 소거 속도, …)
    - 의사난수가 아닌 다른 것으로 fill하려면
      - /dev/zero

mkfs

- mkfs
  - 파일 시스템 만들기 명령어
    - 즉, 포맷
    - `mkfs.ext4` 혹은 `mkfs.ntfs`와 같은 방법으로 사용
    - 각각의 파일시스템별로 서로 다른 명령어로 취급됨 → 각각의 man page 참고
  - `sudo mkfs.nfts -q /dev/sdb3`
    - /dev/sdb3 파티션을 NTFS 파일 시스템으로 빠른 포맷
      - 빠른 포맷: 파티션 구조를 만든 후, 검사하지 않음

shred

- shred
  - (HDD에서) 특정 파일 소거 명령어
    - 특정 파일이 저장되어 있던 섹터를 파악하여 해당 섹터를 몇 번 덮어쓰기함
    - 디스크나 파티션 단위가 아니라 섹터 단위로 덮어쓸 때 유용
  - `shred -uvz -n 2 ~/the_file.txt`
    - 지정된 파일을 두 번 랜덤으로 덮어쓰기하고(-n 2),
      0으로 덮어쓰기해서 소거했다는 사실을 숨기고(-z),
      그 파일을 삭제하되(-u),
      과정을 자세히 보여주기(-v)

hdparm

- hdparm
  - 디스크 관리를 위한 명령어
    - 디스크 암호화 및 소거를 위한 옵션 제공 (--security-erase)
    - SSD를 소거할 수도 있음
  - https://ata.wiki.kernel.org/index.php/ATA_Secure_Erase
    - Secure erase 기능을 사용하기 위한 가이드
    - USB로 연결된 장치에 대해 수행하지 않을 것
  - 디스크 관리 유틸리티로 diskpart 등도 존재
    - diskpart> clean all
      - 장치를 제로필하여 청소

Hand over a laptop

- 컴퓨터 양도
  - 2020년 8월…
    - 컴퓨터를 교체하면서 기존 컴퓨터 (LG 노트북, Windows 사전 설치)을 양도하게 됨
    - ⌘+R → diskmgmt.msc → 복구 파티션 (사전 설치 복구 이미지) 존재
      - 디스크를 완전히 밀어버릴 수 없었음. 기존에 나누어 놓은 파티션과 자동 생성 Windows 복구 파티션을 삭제하고, 하나로 합침 (파티션 확장)
    - Ubuntu Live USB를 준비(Rufus), ‘Try ubuntu’로 부팅
      - 하나로 합친 파티션이 /dev/sdb3으로 인식됨
      - dd if=/dev/urandom of=/dev/sdb3 bs=4096
        - random fill, zero fill 번갈아가면서 각 2회씩 수행. 각각 80MiB/s, 130MiB/s 정도
      - mkfs.ntfs –f /dev/sdb3

Conclusion

- Antiforensic
  - 민감한 정보를 완전히 삭제하는 것
  - 현대 HDD의 소거를 위해서는 2-pass 정도면 충분
    - 특정 파일의 소거는 shred, 파티션/디스크의 소거는 dd
    - random-fill은 /dev/urandom, zero-fill은 /dev/zero
  - SSD의 소거는 제조사 툴 이용

Q&A

wheel seminar