디지털 포렌식 가이드라인

(2022.10)

성신여자대학교 HASH

1 하드 디스크 드라이브의 종류(HDD, SDD)

1.1 HDD란

하드 디스크란 컴퓨터 내장 보조 기억장치이다. 주 기억 장치를 보조하는 역할을 하며 휘발성(데이터 저장 x)인 주기억장치와는 달리 비 휘발성이다. 가장 대중적이고 저렴한 저장소이다.

1.2 HDD의 구성

전원 커넥터 – 하드디스크에 전원을 연결한다.

데이터 커넥터 – 하드디스크와 컴퓨터 사이의 데이터를 전송해주는 단자이다.

헤드 – 데이터를 저장, 삭제 또는 정보를 읽는 역할을 수행한다. 플래터는 양면으로 이루어 졌기 때문에 정보도 양쪽에 존재하므로, 따라서 일반적으로 헤더의 수는 플래터의 수의 2배정도 존재하여 정보를 읽는다.

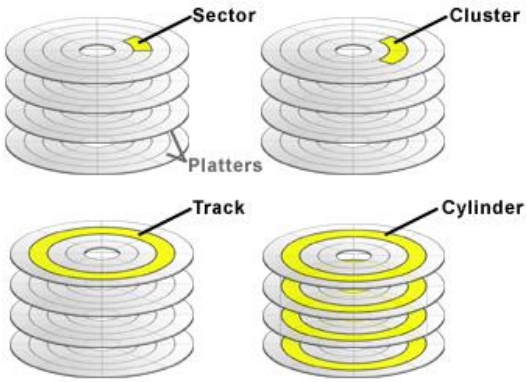
액추에이터 (헤드 구동 장치) – 헤드를 데이터가 있는 곳으로 움직이는 역할을 수행한다.

플래터 – 실제로 데이터가 저장되는 곳이다. 비 자성체은 비금속 원판 표면에 자성체인 산화 금속막을 양면에 도장한 것으로 해당 금속의 막을 논리적으로 나눈 후 위치를 지정하면 데이터 저장이 가능하다.

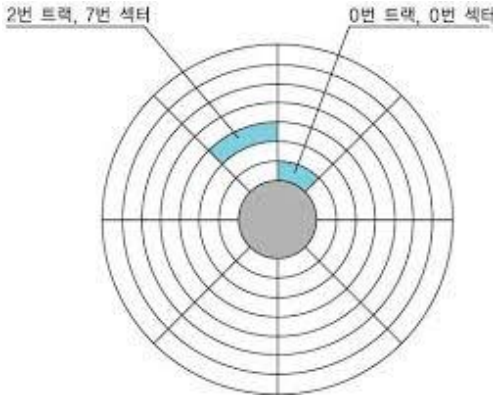
스핀들 – 플래터를 돌려주는 역할. 플래터가 회전할 수 있도록 모터와 직접 연결된 축이다.

회로 기판(PCB) – HDD 하부에 존재. PCB에는 여러 부품들이 부착되어 있음. 회로 기판은 방열/수리 등의 목적으로 노출된 형태가 많아 떨어트리거나 물을 쏟으면 바로 고장남으로 각별한 주의가 필요하다.

실린더



다수개의 플래터의 트랙을 수직적으로 관통하는 3차원 적인 스택을 말한다.



트랙, 섹터 – 하드 디스크 기록 단위의 하나로 동심원으로 구획된 구역 하나하나를 트랙(원)이라 칭하고 그 트랙들은 다시 섹터(원을 잘라놓은 조각)로 나뉘게 된다.

클러스터 – 섹터의 그룹이며 도스에 의해 인식되는 최소 기억 단위이다.

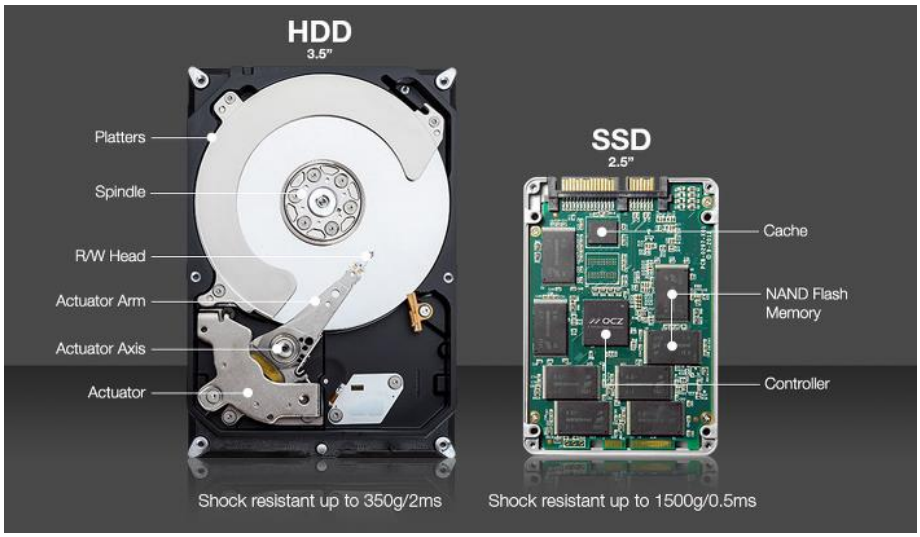
1.3 하드 디스크 작동 원리

하드디스크의 자성 물질로 덮인 플래터를 회전시키고, 그 위에 헤드를 접근시켜 플래터 표면을 자기 배열을 변경하는 방식으로 데이터를 읽거나 쓴다.

헤드는 실제로 플래터와 접촉을 하고 있는 것이 아닌, 표면에 살짝 떠있는 상태로 데이터를 읽거나 씀으로 하드디스크가 동작하는 도중 외부의 충격이나 전원이 차단되면 헤드가 플래터의 표면을 긁어 고장낼 수도 있다.

또한 자성 물질로 데이터를 기록하는 플래터의 특성 때문에 하드디스크 주변에 자석이 있다면 기록된 데이터가 손상되기도 한다.

1.4 SSD (Solid State Drive. Soild State Disk)



하드디스크 드라이브와 비슷하게 동작하면서도 기계적 장치인 HDD 와 달리 반도체를 이용해서 정보를 저장하는 최신 보조 기억 장치이다.

2. HDD와 SDD의 차이

HDD

- 하드디스크는 내부에 배치된 플래터에 자기장으로 데이터를 입력하는 저장 장치이다. (물리적 방식)
- 소음 발생, 소비 전력 높음, 발열 문제를 수반한다는 단점이 존재한다.
- SSD보다 데이터 처리 속도가 상대적으로 느리다. (플래터 돌아가는 속도의 한계와 데이터를 저장하기 위해 데이터가 저장된 위치로 헤드를 옮기는 시간이 소요되기 때문)
- 물리적으로 구성되어 있기 때문에 내구성이 약하다. 따라서 떨어트리는 등의 사고로 부품이 손상되면 복구가 힘들다.
- 휴지통으로 파일 삭제해도 플래터에 그대로 정보가 남아있다. 삭제된 정보는 플래터의 물리적인 영역이 여러 번 재사용 될 때까지 남아있는데, 몇 개월에서 최대 몇 년이 소요된다.
- 파일을 완벽하게 지우고 싶다면 삭제 전용 프로그램을 사용하여 플래터 위에 남아있는 데이터를 수차례 덧씌워야 한다. 이 경우 원본 데이터와 상관 없는 값을 덧씌우기 때문에 복구 가능성은 없다.

SSD

- 플래시 메모리에 데이터를 저장함으로 물리적인 정보가 남지 않는다.
- 데이터 읽기/쓰기 속도는 HDD에 비해 엄청나게 향상된 모습을 보인다.
- 모터가 없으므로 소음이 없고 소비전력과 발열도 적다. 또한 내부에 움직이는 부품이 없기 때문에 외부 충격 때문에 손상될 가능성도 낮다. (HDD의 단점 개선)

- 데이터를 삭제할 경우 완전 소멸되므로 값을 덧씌울 필요도 없고, 복구 또한 불가능하다.
- 데이터를 삭제 시 바로 사라지면 실수로 삭제한 데이터의 복구 가능성이 없어지기 때문에, SSD 또한 일정 시간 이상 데이터 유지하는 특징이 있다. 이후 일정 기간마다 데이터를 정리하는 트림(TRIM)기능이 동작하면 데이터를 완전히 삭제한다.
- 데이터를 완벽하게 지우고 싶다면, 데이터를 휴지통으로 보내 지운 후 윈도우의 드라이브 조각 모음 및 최적화 실행하여 SSD 최적화를 하면 데이터가 완전히 사라져 복구가 불가능하다.

3. SSD, HDD 삭제된 파일 복구 가능한 경우와 복구 불가능한 경우

3.1 복구 가능한 경우

데이터를 시각적으로만 지웠을 경우(ex. 휴지통) 물리적으로는 데이터가 아직 존재함으로 복구 가능

3.2 복구 불가능한 경우

삭제된 데이터 위에 다른 데이터를 덧씌웠거나 SSD의 경우 드라이브 최적화를 통해 포맷한 경우 복구 불가능

4. 복구 방법

4.1 TestDisk (무료)

TUI(Text-based User Interface) 기반으로 명령 프롬프트를 통해 조작해야 한다는 불편함이 있다.

복구 과정: https://postiveemblem.tistory.com/188 (직접 실습해보면 좋을 듯)

https://gyou-story.tistory.com/9

다운로드 주소: https://www.cgsecurity.org/wiki/TestDisk_Download

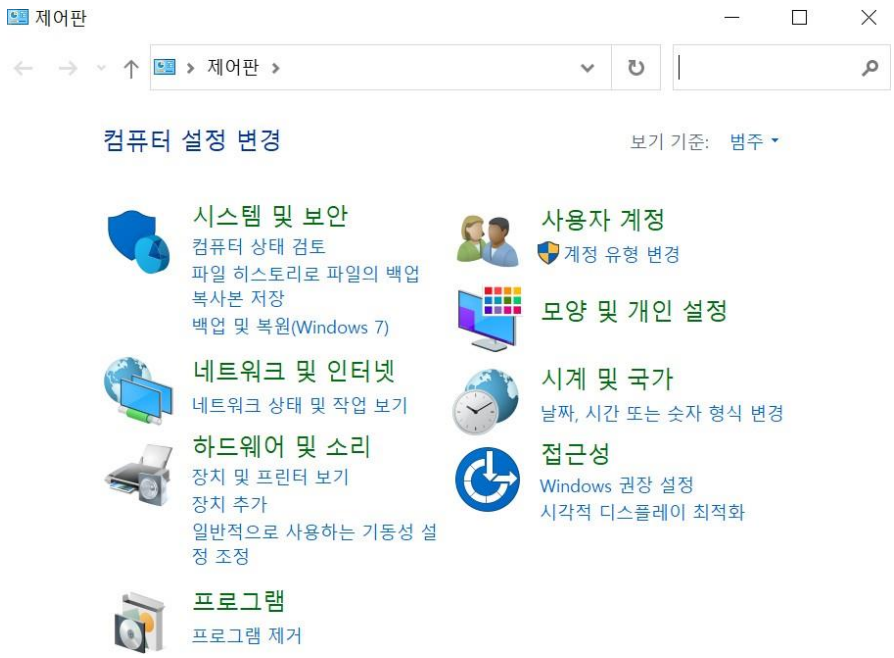
파일 다운로드 후 압축 해제를 하여 폴더 내에 있는 "testdisk_win.exe"를 실행한다. 해당 프로그램 실행 시 알 수 없는 프로그램이라고 나와도 무시하고 실행하면 된다.

단점: 포맷을 진행한 뒤 아무 자료도 저장하지 않은 디스크만 쉽게 복원 가능함으로 실수로 삭제했을 시 바로 복원 작업을 시작해야한다.

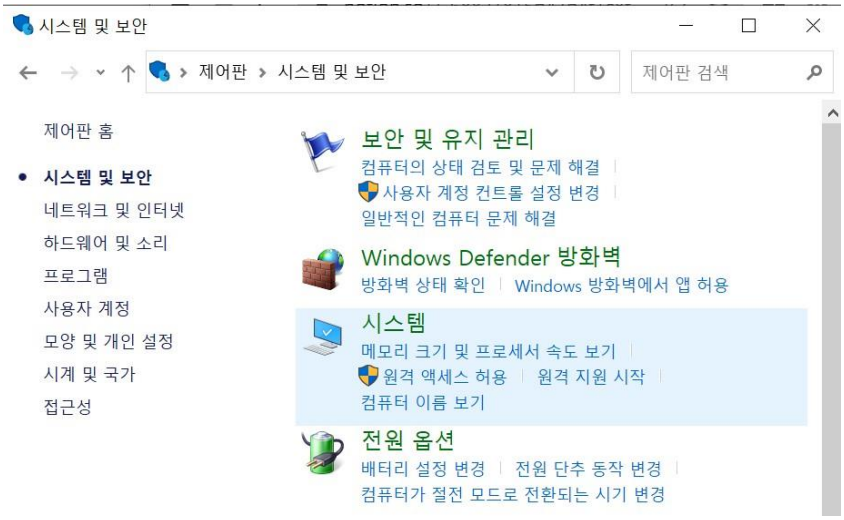
4.2 윈도우 시스템 복원 방법

Windows에서 시스템 복원 활성화

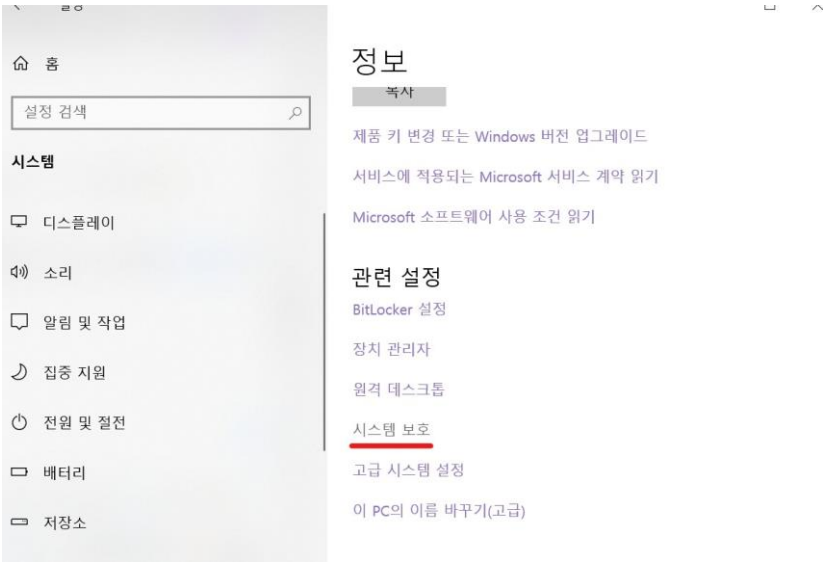
1. 제어판을 연다



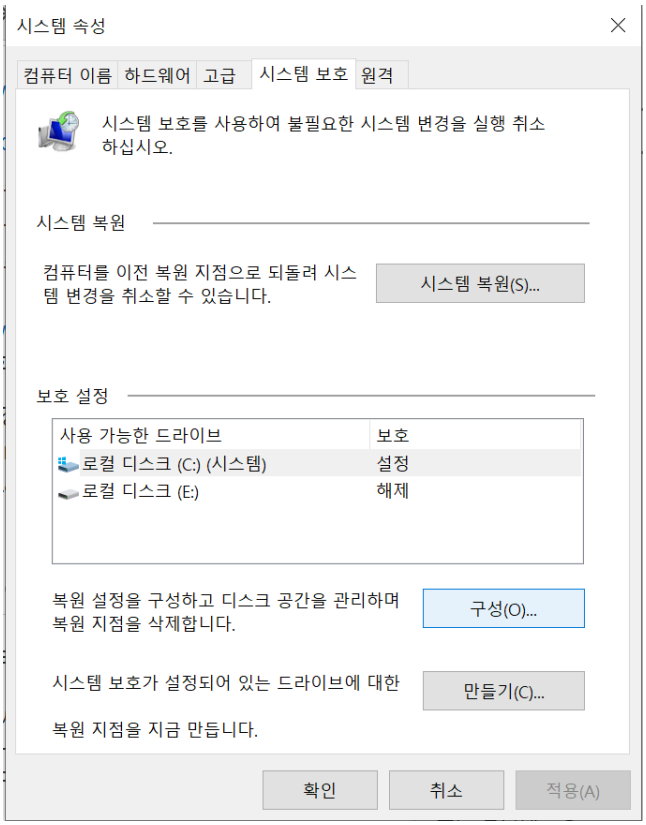
2. '시스템 및 보안'을 선택한 뒤 '시스템을 누른다.



3. '정보'창에서 '시스템 보호'를 선택한다.



4. '구성'을 누른 뒤 복원 설정의 '시스템 보호 사용' 옵션을 선택하고 적용한다.



+) 시스템 복원을 하고 싶다면 3번 단계 이후 창에서 '구성'이 아닌 '시스템 복원' 탭을 누른 뒤 복원할 지점을 고른다.

시스템 복원을 사용하지 못하는 경우

- 컴퓨터 바이러스, 해킹 툴에 감염되었을 경우

이런 종류의 프로그램은 시스템 자체를 건드리는 경우가 많지만 이 프로그램의 감염 경 로는 대부분 사용자 라이브러리에 위치하기 때문에 시스템 복원을 해도 시스템만 복원될 뿐 시스템을 바꾸게 만드는 소스는 영향을 받지 않는다. 또한 이런 프로그램은 복사 본을 하드디스크나 SSD에 뿌려 놓는 경우가 많아 재감염될 가능성이 높다. 더불어 일부 랜섬웨어는 시스템 복원 자체를 못 쓰게 만들기도 한다.

- 파티션 이상

  파티션이 망가지면 인식이 안 되기 때문에 한 번 정해진 파티션을 여러가지 프로그램을 이용해 억지로 크기를 늘릴 경우 불안정해지는데 이런 경우 시스템 복원은 의미가 없다. 시스템 복원을 하는 기반 자체가 망가진 것이기 때문. 해결책은 파티션을 지우고 처음부 터 다시 만든 다음에 포맷하고 재설치 하는 것이 가장 좋다.

- 저장 매체 이상

  HDD, SSD, USB 메모리 등의 저장 매체 자체가 고장난 경우 복구 및 수리가 불가능하 므로 새 제품으로 교체해야 한다. 이 경우 내부 자료는 지워지기 때문에 데이터를 복구하고 싶다면 다른 방법을 이용해야 한다.

- 공장 초기화를 원할 경우
  윈도우를 설치하자마자 윈도우에서 제공하는 시스템 백업을 해놓으면 모바일 기기처럼 원할 때 간단히 공장 초기화 할 수 있을 거라 생각하는 경우가 많지만, 시스템 복원은 그 냥 덮어쓰기일 뿐 지우기 작업은 하지 않는다. 시스템 복원을 해도 프로그램 폴더에 가 보면 이전에 설치한 프로그램이 그래도 남아 있다.

4.3 FTK Imager(무료)

FTK Imager 설치 (https://accessdata.com/product-download-page)

해당 방법은 FTF Imager로 복구하고자 하는 파일의 이미징을 떠야 파일 복구가 가능하다.

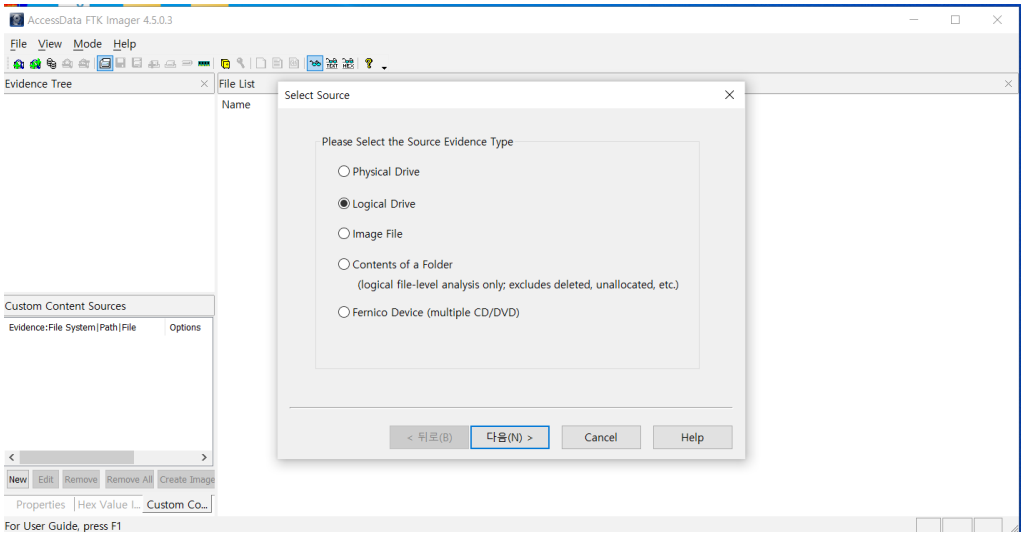
디스크 이미징이란? 하나의 드라이브를 하나의 파일로 제작하는 것을 말한다.

이미징을 뜨기 위한 필수 요소: 우리가 원하는 파일을 이미징을 떠 다른 드라이브나 이동식 디스크로 옮겨야 복구가 가능하기 때문에 이미징을 뜨고자 하는 디스크(C 드라이브, USB 등) 이외의 드라이브나 이동식 디스크가 필요하다.

SSD 파티션이 하나인 경우 파티션을 C, D 드라이브로 나누어 주어야 복구가 가능하다.

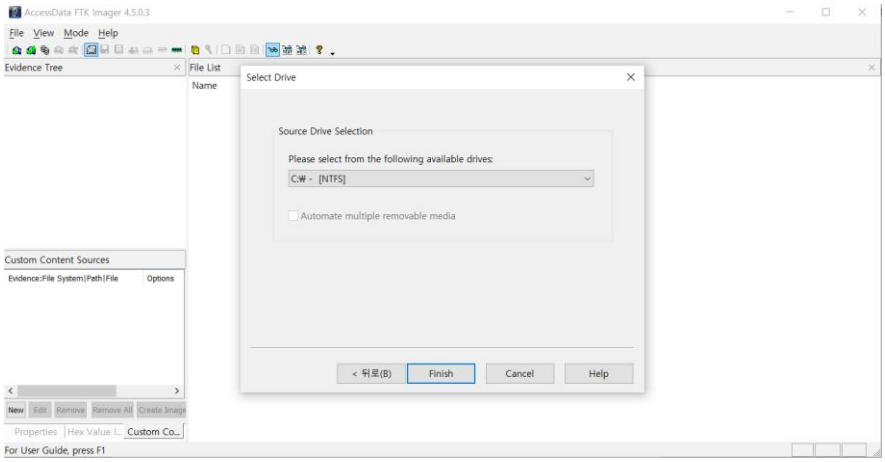
파티션을 나누는 방법: https://coding-factory.tistory.com/492

이미징 뜨는 방법

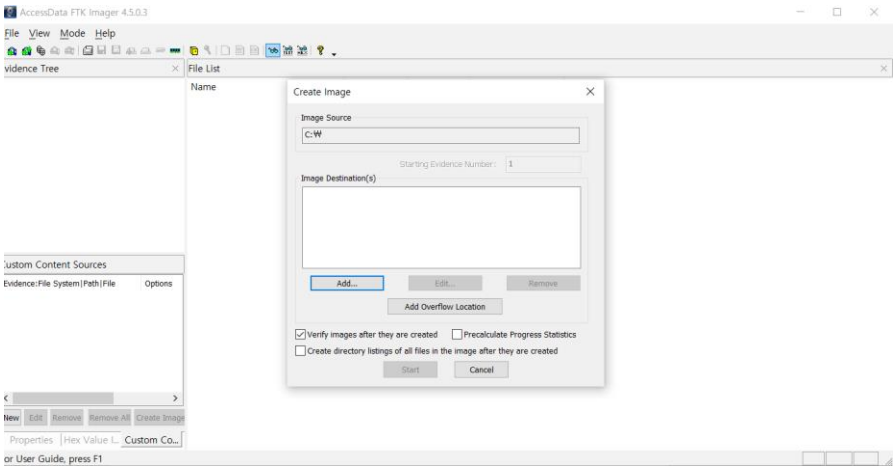


1. FTK imager를 들어가 Create disk image 버튼을 누른다.

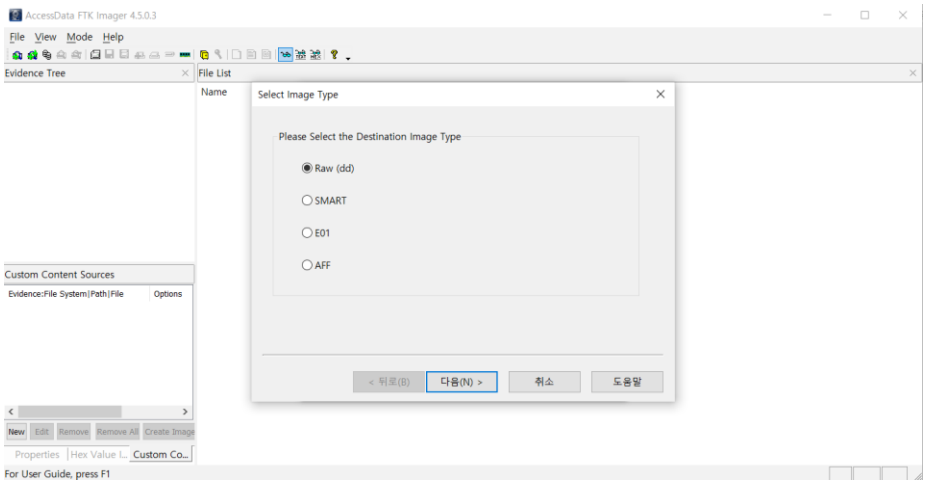
   만약 SSD나 드라이브 단위의 분석을 하고 싶다면 Physical Drive, SSD 내의 C:, D: 단위의 분석을 하고 싶다면 Local Drive를 클릭한 후 다음을 누른다.



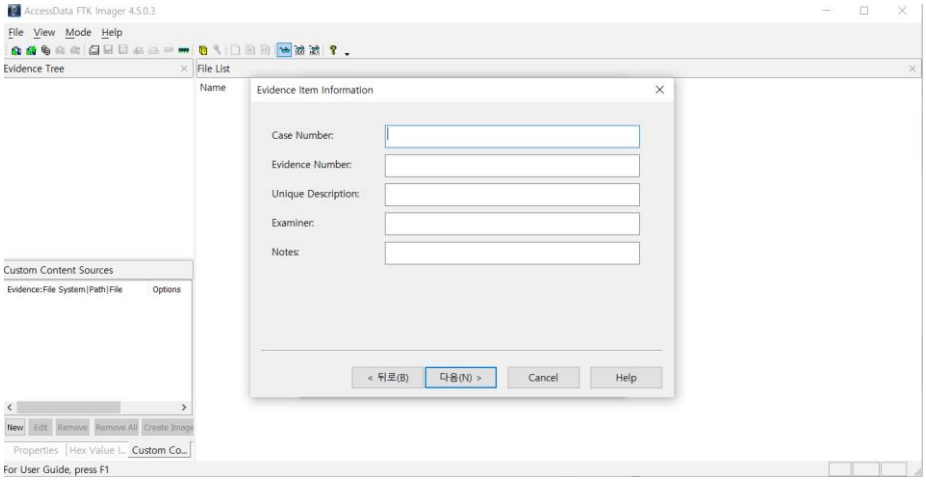
2. 복구를 원하는 드라이브를 선택한 후 Finish를 누른다.



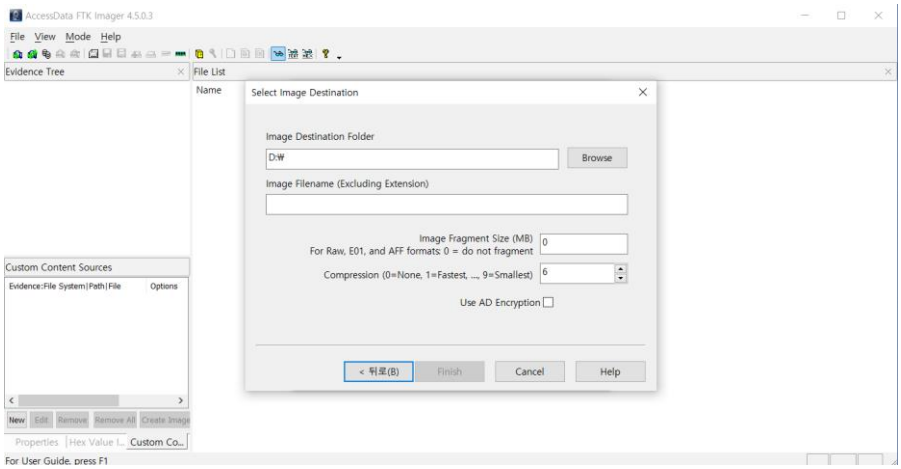
3. 해당 창에서 Add를 누른다. 이 창은 우리가 이미징 할 파일의 형식과 저장 공간을 설정해주는 창이다.



4. Image type를 선택하는 창이다. 대체로 Raw(파일 그대로의 형태) 혹은 E01를 선택한다. E01이 조금 더 압축된 형식이므로 E01를 선택해주도록 한다.



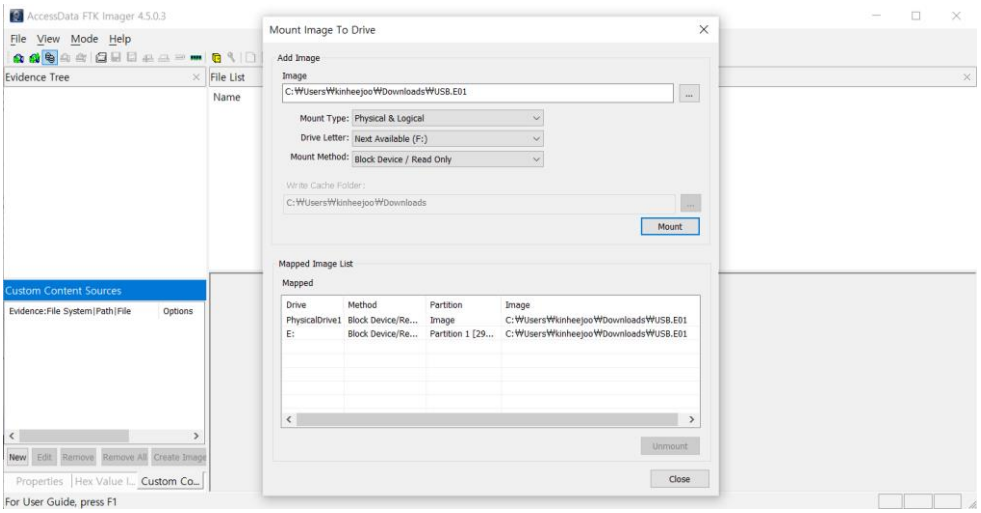
5. 해당 창은 실제 수사에서 케이스를 분류할 때 입력하는 것으로 입력하지 않아도 된다.



6. Image Destination Folder은 이미징 할 파일을 저장하는 장소로써 우리가 이미징 할 드라이브와 다른 드라이브를 선택해준다.

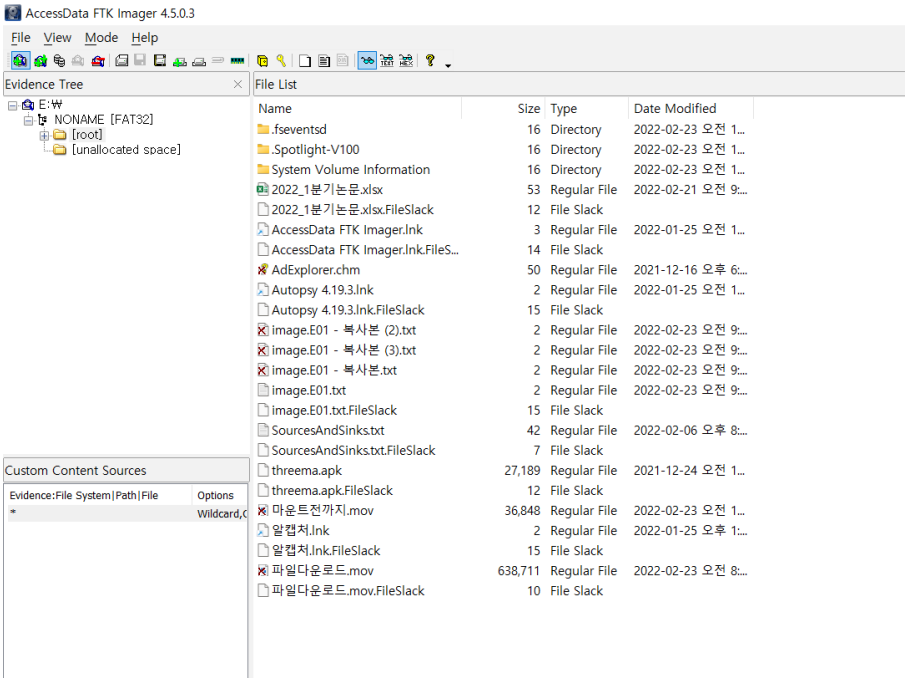
Image Filename은 우리가 이미징 할 파일의 이름을 정해주는 것으로 이름을 입력해주면 된다.

Image Fragment Size는 이미지를 쪼개는 정도를 말하는 것으로 0을 입력해줌으로써 파일을 쪼개지 않고 분석해주도록 하겠다. 해당 창을 다 입력했다면 Finish를 누르고 디스크 이미징을 시작하도록 한다. 디스크 이미징은 용량이 크기 때문에 시간이 오래 걸리는 점을 유의하자.



7. FTK imager를 통해 디스크 이미징 한 파일인 USB.E01을 드라이브에 마운트 한다. (Mount 버튼 클릭)

마운트란? 디스크 이미징을 통해 만든 하나의 파일을 다시 드라이브로 만드는 것으로 저장되어 있던 파일 그대로 복구하기 때문에 모든 파일 확인 가능하다. (이미징의 반대 개념)

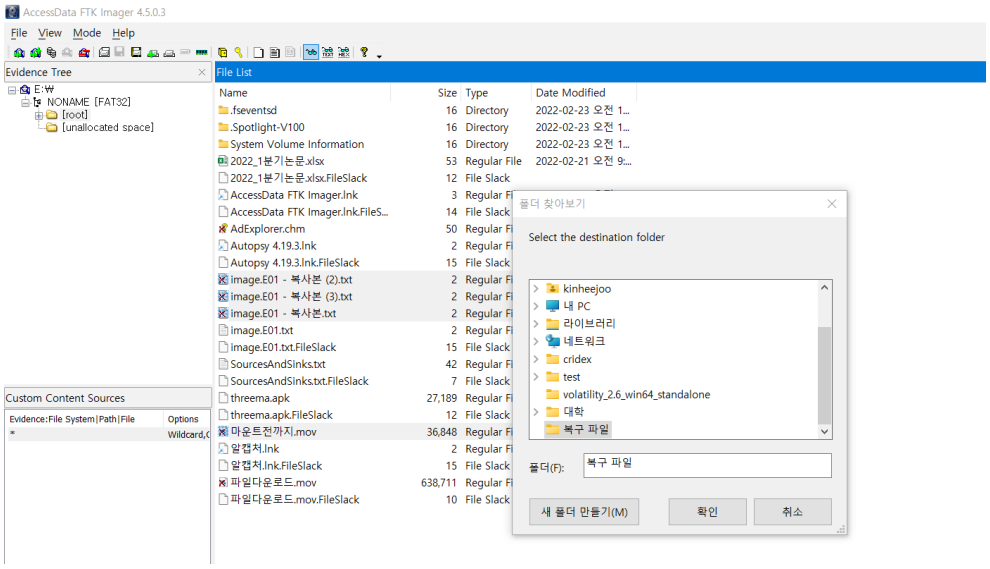


8. 디스크 마운트 후 복구한 파일을 FTK imager의 Evidence Tree에 불러올 수 있다.

Root 파일: 디스크 이미지 안에 들어있는 파일을 다 보여주는 것

파일 옆에 x가 되어있는 파일: 삭제된 파일, 파일을 복구해도 삭제된 파일은 보이지 않는다.

하지만 FTK imager로 복구하니 삭제 파일도 볼 수 있었다.

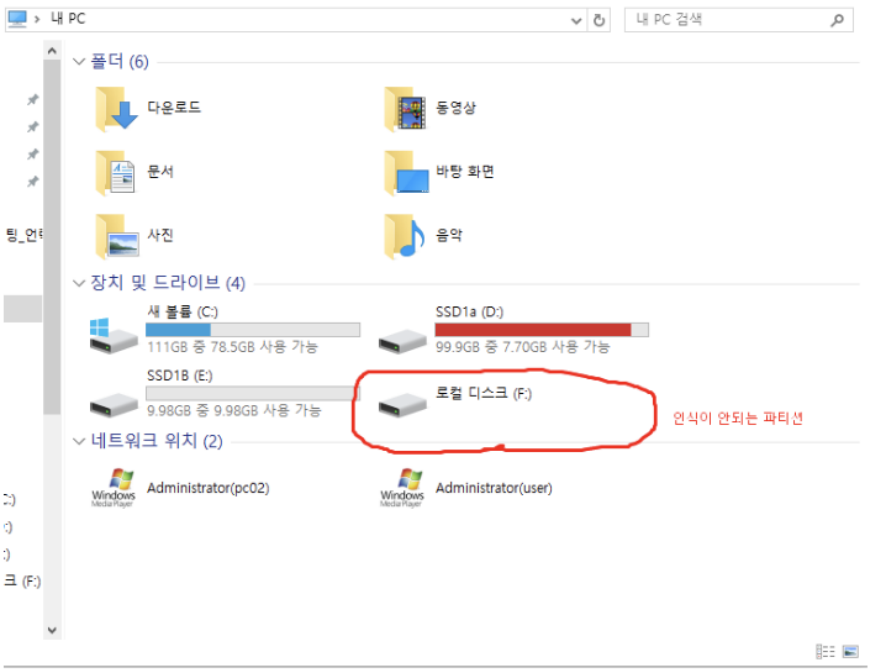


9. 오른쪽 마우스를 클릭해서 Export file을 누를 누른 후 폴더 지정하고 확인을 누르니 파일이 복구되었다.

Image.E01 파일과 복사본들은 2byte로 매우 작으므로 빈 파일이다.

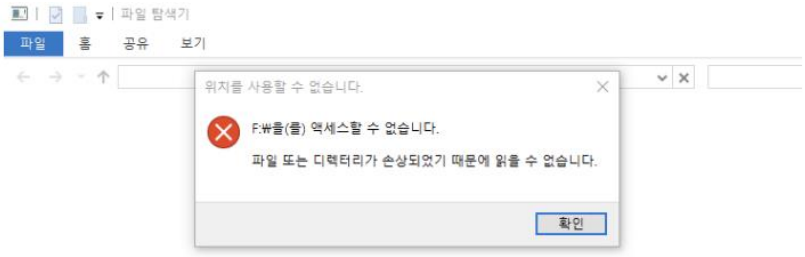
마운트전까지.mov 는 파일 크기가 큰 만큼 동영상인 것을 확인할 수 있다.

4.4 MiniTool Data Recovery로 복구하기



1. 인식이 안되는 F 디스크

SSD 디스크이며 파티션을 3개로 나눠 쓰고 있음. SSD1C 라고 네이밍 한 데이터 백업 디스크이므로 무조건 복원해야 한다.



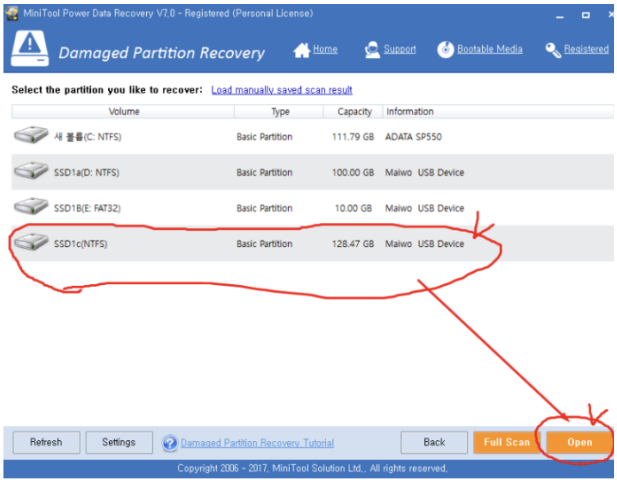
2. 포맷해야 읽을 있다고 뜬다.

MiniTool Data Recovery 툴을 사용해서 복구한다.

https://www.powerdatarecovery.com/

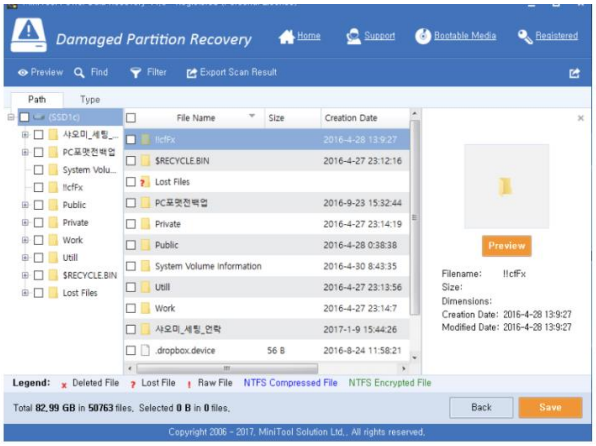
➔ 해당 사이트

➔ 해당 사이트에서 Free 에디션을 다운 받는다. 1기가까지는 무료 복원 가능 그 이상은 유료

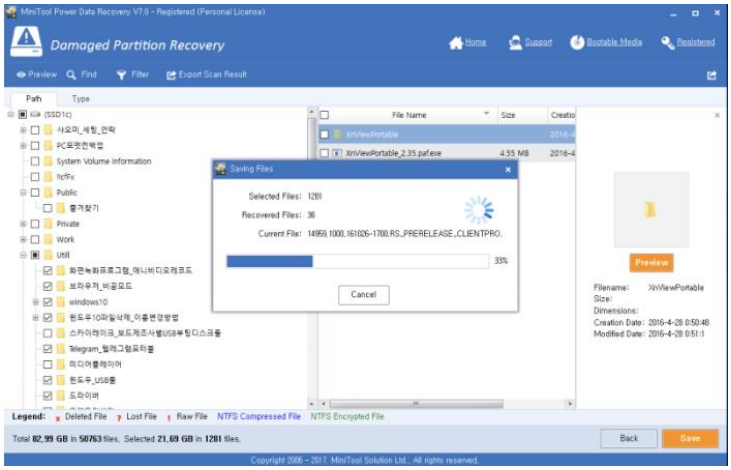


A. 위 사진처럼 파티션 리스트가 보인다. 그중 손상된 파티션을 선택 한 후 open 버튼을 누른다. Full Scan 버튼은 하드디스크가 아주 심각하게 손상되었을 때 이용하면 된

다.



B. 윈도우에서 엑세스 되지 않았던 파티션 속의 모든 데이터가 보임. 이미 정보가 손상된 파티션은 더 이상 이용 불가능하다. 포맷을 한 후 안전하게 사용해야 함. 그러기 위해서는 데이터 복원을 먼저해야 한다.



C. 복원할 파일을 모두 체크한 후 하단의 Save 버튼을 누른다.

저장할 위치를 묻는 팝업이 나오고 다른 파티션을 선택하면 된다. 복원할 데이터 선택 후 Save를 누르면 저장할 위치를 저장하면 지정된 곳으로 파일들이 모두 복사된다.

1 메모리 카드

1.1 메모리 카드란

메모리 카드는 플래시 카드라고도 하며 플래시 메모리 기반의 디저털 데이터 저장 장치이다. 디지털 카메라, MP3 플레이어, 휴대전화, 노트북 등에 사용되어 용량을 증설하거나 데이터를 옮기는 데 사용한다. 자가 기록 매체인 디스켓과 같이 데이터를 쓰고 지울 수 있고 전력이 없어도 내용이 유지된다.

메모리 카드의 종류를 가장 큰 개요로 나눠보자면 다음 표와 같다.

메모리 카드	
외장형	Secure Digital(MiniSD/MicroSD), CompactFlash(Microdrive), 메모리 스틱, UFS 카드, XQD, CFexpress, xD 픽처카드, 스마트 미디어
내장형	MMC(eMMC), UFS

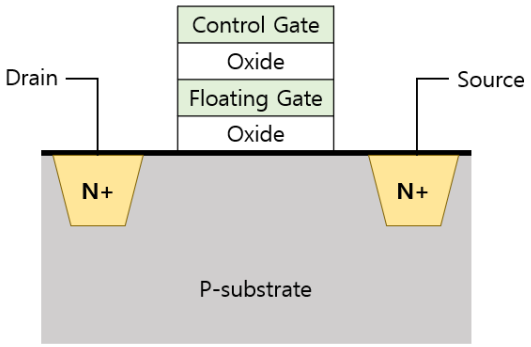
우리가 아는 가장 흔히 접해본 SD 카드도 외장메모리에 속한다. SD 카드는 카메라에서 주로 많이 사용되고 microSD 카드는 안드로이드 스마트폰에서 주로 사용되고 있다.

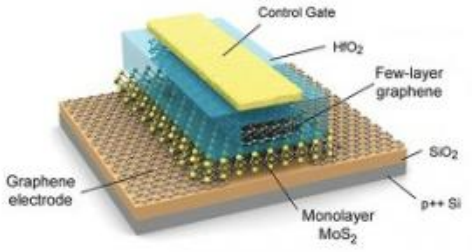
1.2 메모리 리더

메모리 리더는 메모리 카드를 컴퓨터에 연결하여 파일을 볼 수 있게 하는 장치로 컴퓨터 안에 내장되어 있거나 외장 리더를 이용하면 볼 수 있다. 대부분의 메모리 카드를 장착할 수 있도록 규격도 다양하다.

2 메모리카드의 동작 원리

플래시 메모리 구조





플래시 메모리는 플로팅 게이트 트랜지스터로 구성된 각 셀에 데이터를 저장하는 방식으로 작동된다. 플로팅 게이트(Floating Gate)에 전자를 채우거나 비워 데이터를 기록하거나 지우는 원리이다. 이때, 플로팅 게이트는 산화막(Oxide, 절연막)으로 둘러싸여 있어 컨트롤 게이트에 충분한 양전압을 가하면 전기장의 영향으로 일부의 전자가 터널링 산화막을 통과하여 플로팅 게이트로 들어간다. 이러한 작업을 데이터 '쓰기'라고 한다. 반면 반도체 기판에 충분한 양전압을 가하면 플로팅 게이트에 갇힌 전자를 비울 수 있는데 이를 데이터 '지우기'라고 한다. 마지막으로 플로팅 게이트에 채워진 전자의 양(전하량)을 측정하는 것을 데이터 '읽기'에 해당한다.

3 메모리 카드의 손상

가장 대중적으로 사용되는 SD 카드를 기준으로 손상된 메모리 카드의 증상을 알아보고자 한다. SD 카드가 손상되는 이유로는 물리적인 손상, 파일 시스템의 오류 및 손상, 파일 전송 중 장치에서 SD 카드 제거, 여러 장치에 동일한 메모리 카드 사용, SD 카드 무단 제거, 바이러스 감염이 있다. 이처럼 무언가로 작동이 방해받고 있다면 비정상적으로 작동한다. 그때 다양한 증상들이 SD 카드에 나타나는데 이는 SD 카드가 손상되었음을 의미한다. 그러한 증상들을 초기에 잘 발견한다면 메모리 카드 속 데이터 손실의 위험을 줄일 수 있다. 손실되기 전 중요한 데이터들을 미리 다른 곳으로 옮길 수 있기 때문이다. 가장 일반적인 증상은 다음과 같다.

- 누락된 데이터

SD 카드가 손상되기 바로 전에 알 수 있는 경우로 사진, 비디오, 노트, 시트 또는 다른 데이터 등이 누락되었음을 발견할 수 있다.

- 카드가 인식되지 않을 때

SD 카드가 인식되지 않는다는 메시지는 SD 카드가 데이터 손상을 겪고 있다는 뜻이다.

- 오류 메시지

SD 카드를 삽입하고 활성화하려고 시도할 때 '액세스 거부' 또는 '포맷이 되지 않는 카드입니다'와 같은 경고창이 띄워지는데 이는 카드가 손상되었다는 신호이다.

- 알 수 없는 파일

바이러스가 침입하여 카드를 손상시키면 파일이 열리지 않거나 삭제되지 않는 파일로 표시된다.

- 읽거나 쓸 수 없을 때

카드를 읽거나 쓰는데 문제가 있다. 이는 손상되었다는 것을 의미한다.

- 장치 오작동

손상된 SD 카드가 연결된 장치는 즉각적으로 오작동하게 된다.

- 빈 SD 카드

데이터가 손상된 SD 카드는 장치에 비어있게 표시될 수 있다.

4 손상된 메모리 카드 사전 확인 및 복구프로그램 없이 복구하는 방법

- 어댑터/카드 리더 혹은 USB 포트 변경 카드리더는 정교한 장치로 손상되기 쉬어 메모리 카드가 다른 카드 리더에서 작동하지는 우선 확인한다. 또한 다른 USB 포트를 사용해 포트가 올바르게 작동하는지 확인해본다.
- 다른 장치/PC에서 카드 사용해보기 시스템이 카드를 인식하지 못하는지, 카드 자체의 손상인지 확인해본다.
- 메모리 카드가 쓰기 보호가 되어 있는지 확인하기 카드에 쓰기 보호가 되어 있다면 새 데이터를 쓰기, 삭제할 수 없고 포맷 역시 할 수 없다.

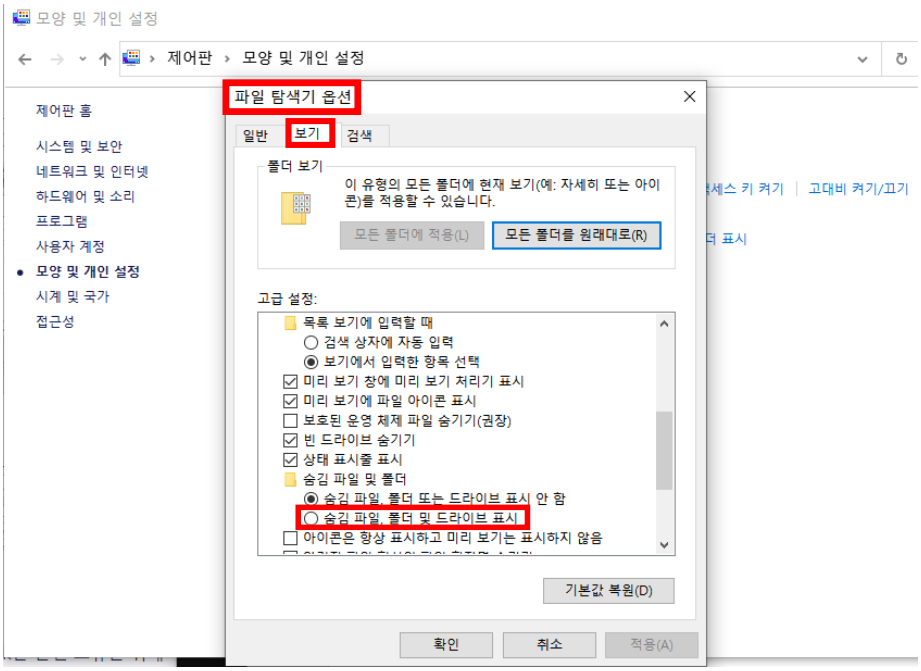
위 사항들을 사전적으로 확인하고 그 다음 절차인 복구 프로그램 이용 없이 손상된 메모리 카드 복구하는 법으로 넘어간다.

4.1 체크디스크(chkdsk) 실행하기

포맷 메시지, 매개변수 오류, 액세스 오류 등의 논리적인 파일 시스템 손상시에 무료로 활용할 수 있는 툴로 체크디스크가 있다. Chkdsk는 microsoft의 windows 운영체제에 사용되는 명령어로 하드디스크 또는 메모리 등의 파일시스템의 무결성 상태를 확인할 수 있고 파일 시스템의 오류를 수정할 수 있다. 즉, 손상된 SD 카드를 수정할 수 있는 간단하고 빠른 응답 명령 유틸리티가 있다. 손상된 SD카드에서 파일을 수정하고 복구하도록 작업할 수 있다. 단계별로 정리하자면 다음과 같다.

4.1.1 손상된 SD 카드 내 숨겨진 파일 확인

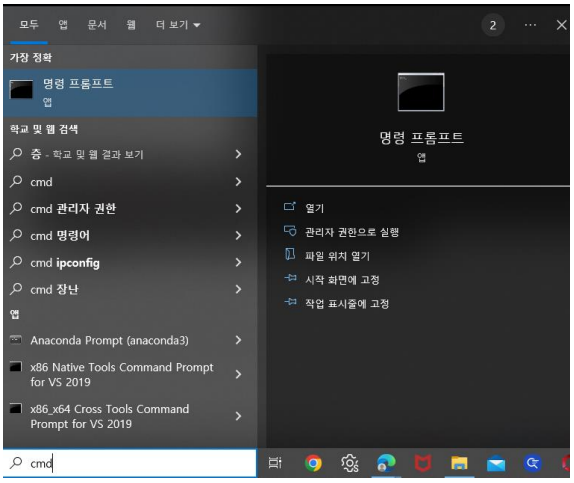
I. 파일 탐색기 > 도구 > 폴더 옵션 > 보기 탭을 연다.



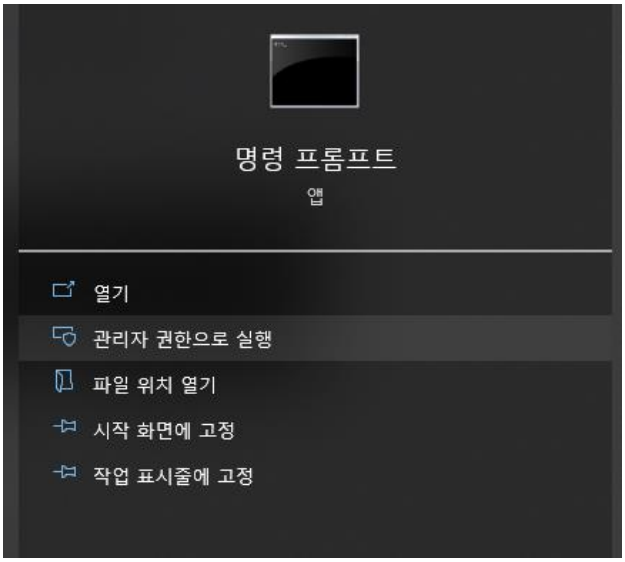
II. 숨겨진 파일, 폴더 및 드라이브 표시 체크 박스를 선택하여 숨겨진 파일을 지금 볼 수 있는지 확인한다.

4.1.2 Chkdsk 명령을 통해 오류 확인

I. 작업 표시줄에서 CMD를 입력해 명령 프롬프트 창을 띄운다.

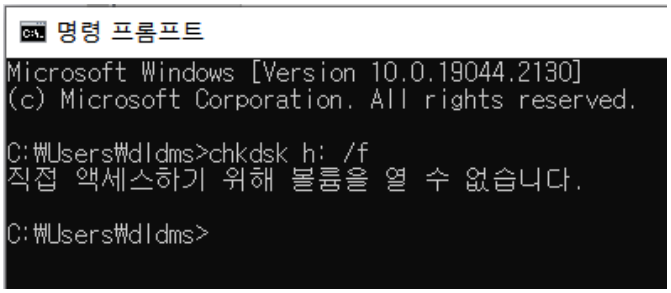


II. 관리자로서 실행을 선택한다.



III. Chkdsk X: /f를 입력하고 SD 카드에 할당된 문자로 X를 교제한다.

(SD 카드가 H: 드라이브면 chkdsk h: /f로 입력해야 한다.)



IV. Enter 키를 누른다.

V. Hkdsk 명령을 완료한다. SD 카드에 들어있는 데이터의 양에 따라 시간이 소요된다,

4.2 손상된 SD 카드 포맷하기

다음 방법은 손상된 SD 카드를 복구할 수 있고 대부분의 손상 문제시 활용해볼 수 있는 방법이다.

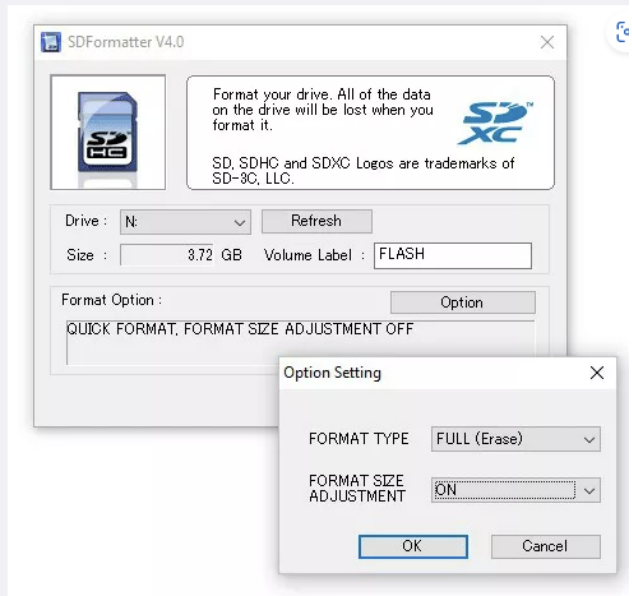
I. SD 카드를 PC 노트북에 연결한다.

II. 내 컴퓨터/내 PC를 더블클릭하여 Windows 탐색기를 연다.

III. 장치 및 드라이브에서 SD 카드를 우클릭하고 포맷을 선택한다.

IV. 파일 시스템 상자를 클릭해 다음 중 하나를 선택한다. – NTFS, FAT32, exFAT 중 원하는 형식을 선택할 수 있다

V. 시작 버튼 누른다.



[2022] 포맷없이 손상된 SD 카드를 고치는 13가지 방법 (tenorshare.com) ← 이곳에서 10가지 해결 방안을 제시하고 있는데 다 넣기보다 몇 개만 골라서 넣고 싶은데 어떤 걸 뽑아서 넣는게 좋을 까요?..아니면 효정님 8주차 자료 바탕으로 다 넣어야 할까요? 아니면 깔끔하게 복구 프로그램 이용해서 복구하는 법만 제시할까요.?

5 복구 프로그램 이용(4DDIG) – 아래 사이트 참고해서 실습할 예정

준비물: SD 카드, SD 카드 삽입 기기, SD 카드 리더기, 프로그램 다운로드.

[2022] 포맷없이 손상된 SD 카드를 고치는 13가지 방법 (tenorshare.com)

6 그 밖의 SD 카드 손상을 최소화하기 위한 방법

SD 카드를 손상되지 않고 최대한 오랜 기간 좋은 상태를 유지하며 관리할 수 있는 방법이 존재한다. 첫째로 여분의 SD 카드를 구입해두는 것이 좋다. 물론 좋은 SD 카드를 사야겠지만 SD 카드 자체가 얇고 작으며 깨지기 쉬운 플라스틱 조각으로 되어 있기에 일반적인 마모로 인해 쉽게 물리적으로 손상될 수 있다. 따라서 여분의 SD 카드를 구비하여 자주 교채해 가며 사용해야 한다. 둘째로 SD 카드에서의 파일 삭제 방법이다. 카드를 포맷하면 카드 전체가 비워져 새롭고 깨끗한 상태가 되는 반면, 지우기 옵션은 이미지와 비디오 파일만 삭제하고 카드 내부에 저장된 경우 관련 없는 다른 파일은 그대로 둔다. 여러 장치에서 하나의 SD 카드를 사용하게 될 경우를 모두 고려한다면 포맷을 사용해서 메모리 카드 내의 데이터를 삭제하는 것이 더 손상을 낮출 수 있다. 서로 다른 장치 서로 다른 파일 형식과 폴더를 동일한 카드에 기록하여 버그나 파일 손상 등 카드의 오류 위험이 증가하기 때문이다. 마지막으로 SD 카드는 물리적으로 손상되기 쉬운 제질의 형태이기 때문에 내부로부터 충격 흡수를 위해 하드케이스로 된 단단한 SD 카드를 권장한다.

손된 SD카드의 인식오류 문제를 해결하는 방법(초보자도 5분이면) : 네이버 블로그 (naver.com)

사례 및 디지털 증거수집 및 처리를 설문한 결과 분석

〈표 3〉 사건 관련 없는 사생활 정보인지

설문	세부 문항	인원(명)	비율(%)
사건 관련 없는 사생활 정보인지	있다	4	3
	없다	130	97
합계		134	100.0

~~위의 표와 같이 임의 제출 받거나 압수한 증거에서 사건과 무관한 사생활 정보를 본 적이 있는 경우가 65.7%이다. 따라서 증거를 취급하는 수사기관에서 사생활 정보에 대하여 더 세심한 주의의 필요성이 요구된다.~~

〈표 4〉 사건 관련 없는 사생활 정보 처리

설문	세부 문항	인원(명)	비율(%)
사건 관련 없는 사생활 정보 처리	원본 그대로 송치한다.	52	43.3
	삭제한다.	30	49.2
	임의로 보관한다.	23	7.5
합계		134	100.0

~~사건과 관련 없는 사생활 정보에 대하여 어떻게 처리하는지에 대한 설문에서는 위 표와 같이 43.3%가 회신 받은 원본 그대로 송치하고 삭제는 19.2%, 법원의 요청에 대비하여 판결 전까지 증거로써 일시적으로 보관하는 경우가 7.5%에 달한다. 수사가 종료된 이후에는 사생활 정보, 수사 관련 자료들도 삭제해야 하지만 법원에서 사건이 판결 날 때까지 분석 결과를 보관하는 것으로 나타나 증거 보관에 대하여 제도적 보완이 필요함을 알 수 있다.~~

1. [사설] '계엄 수사' 핑계로 참고인 휴대폰 여성 사진 돌려봤다니 - 조선일보 (chosun.com)

   '기무사 계엄 문건'을 수사한 군·검 합동수사단 관계자들이 임의 제출 받은 참고인 휴대전화에서 나온 여성들 사진과 동영상을 불법적으로 돌려보며 '낄낄거렸다'는 수사단 내부 증언이 나왔다고 한다

2. "사생활 보호도 중요" 깐깐해진 디지털 압수수색 (hankookilbo.com) (뭔가 사설 업체보다는 경찰청 사이버 수사대 같은 수사기관과 관련된 느낌)

휴대전화 압수수색: 휴대전화 즉 스마트폰의 압수수색은 컴퓨터 압수수색과 달리 범죄사실과 무관한 정보들까지 노출될 가능성이 크다. 왜냐하면 컴퓨터는 암수수색시 검색어를 돌려서 범죄사실과 관련성 있는 것만 찾는데 스마트폰은 그렇게 검색을 돌리기 어렵고 그러한 경계를 구분하기 힘들다고 한 법조인이 이야기한 바 있다.

검찰에게 스마트폰은 블랙박스이다.

신정아 사건(학력위조사건..2007), 왕재산 사건(간첩행위), 이석기 사건 등에서 휴대전화 압수수색을 둘러싼 충돌이 많았음.

한 검찰 간부는 제3자가 개입하여 예민한 개인정보 및 사생활 침해 우려가 있는 정보는 추리고 나머지만 수사기관에 제공하는 제3의 독립위원회를 만들자는 아이디어도 나온다고 한다. 그러나 수사기관이 보든, 제3자가 보든 개인정보 침해는 마찬가지이기 때문에 그러한 아이디어는 크게 발전하지 못했다.

또 최근 클라우드 포렌식 때문에 아무리 스마트폰을 망가뜨려도 구글, 네이버, 카카오 등은 스마트폰 연락처나 일정, 사진 등 서버에 동기화하는 서비를 제공하기에 아이디 비밀번호만 알면 스마트폰 폐기는 허사가 된다.

3. 디지털 포렌식 과정에서 변호사의 조력을 받아 사생활 노출을 방지

디지털 포렌식 전과정 참여(카촬죄) - 사생활침해 방지 | 로톡 (lawtalk.co.kr)

"디지털 포렌식 전과정에 참여하여 헌법과 형사소송법상 피의자의 방어권을 적극 행사, 영장에 기재된 범위외에 다른 사생활을 침하거나 먼지털이식 수사를 진행하는 것을 방지 "

의뢰인은 술자리에서 즉석만남을 통해 만난 고소인과 잠자리를 하게 되었고 그 후 고소인은 의뢰인이 자신의 연락을 더 이상 받지 않자 카메라 등 촬영을 이유로 형사 고소를 하였습니다.

수사 과정에서 포렌식 절차가 진행되던 중 의뢰인이 변호인을 찾았고 영상을 찍지 않았음을 주장하였습니다. 다만, 전 여자 친구들과는 합의하에 영상을 찍은바 있고, 별도로 야한 동영상을 본 적도 있는데, 혐의와는 전혀 상관없는 과거 영상들 및 인터넷 사용내역이 새로운 사건으로 되거나, 전 여자 친구들에게 확인 연락이 갈까 걱정하였습니다.

이에 파운더스는 **포렌식 전 과정에 참여**하였습니다. 복제 및 분류과정 참여하여 영장에 기재된 날짜와 관련 영상만 보도록 **하였고 과거 자료 등 사건과 무관한 자료로 인하여 모든 개인사가 노출되거나 알려질 염려를 해소**하였습니다. 결국 사건 당일 영상은 나오지 않았고 의뢰인은 **최종적으로 무혐의처분**을 받았습니다.

디지털 포렌식은 수사 단계에서 피의자가 이미 삭제한 증거를 찾아내거나 반대로 사례와 같이 피의자의 억울함을 풀 수 있다는 이점이 있으나 조사 과정에서 피의자의 사생활이 노출되는 등 불이익도 많이 발생하므로 포렌식 수사 시에는 반드시 변호사의 조력을 받아 대처하시기 바랍니다.

끝으로 법률사무소 파운더스에 의뢰하시면 변호사가 직접 포렌식 전 과정 참여하여 의뢰인을 적극적으로 방어하고 사생활이 노출되는 것을 방지하며, 혹시 헌법과 형사사송법상 영장주의 원칙에 반하여 증거조사가 이루어질 우려나 위험이 있다면 최선을 다해 의뢰인의 헌법상 방어권을 행사할 것을 약속드립니다.

1. 파티션

1.1 파티션이란

파티션이란, 디스크 공간을 논리적으로 별도의 데이터 영역으로 분할한 공간을 칭한다. 하나의 디스크를 서로 분리된 여러 개의 디스크처럼 사용이 가능하다. 파티션을 사용하면 한 컴퓨터에 운영 체제를 두 개 이상 설치가 가능하다는 장점도 있다. 나누어진 파티션의 정보를 저장하는 파티션 테이블이 있는데, 해당 테이블에는 최대 4개의 파티션의 정보밖에 저장하지 못한다. 또한, 포맷된 개별 파티션은 컴퓨터의 메모리와 저장공간을 공유한다.

파티션은 크게 주 파티션인 Primary 파티션, 논리 파티션인 Logical 파티션, 그리고 확장 파티션인 Extended 파티션 총 3가지로 나눠볼 수 있다. 디스크를 여러 공간으로 나누어 파티션으로 사용하는 가장 큰 이유는, 편리성으로 볼 수 있다.

1.1.1 Primary Partition

파티션 앞에 부트섹터가 할당되어 운영체제를 설치할 수 있다. 이때, 주 파티션에 운영체제를 설치하게 되면 부트 섹터에 부트레코더를 기록하고, MBR에도 기록한다. 주 파티션은 최대 4개까지로 나누어 사용할 수 있으며, 윈도우의 C, D, E 드라이브와 비슷하다.

1.1.2 Logical Partition

논리 파티션은 메인 메모리 및 기타 리소스의 논리적 분할로, 운영체제 및 관련 어플리케이션의 자체 복사본을 실행할 수 있다. 논리 파티션은 하드디스크의 저장 능력에 따라 사용할 수 있는 개수가 달라진다.

1.1.3 Extended Partition

확장 파티션은 논리 드라이브를 감싸는 벽으로 비유해볼 수 있다. 파티션이라고 정확히 정의하기는 어렵지만 논리 파티션을 사용하기 위해 이용하는 파티션으로 생각할 수 있다. 확장 파티션은 최대 1개만 사용 가능하다.

1.2 파일 시스템

파일 시스템이란, 하드디스크를 알맞게 포맷해서 관리해주는 시스템을 말한다. 한정된 자원을 효율적으로 사용하기 위해 파일과 폴더의 위치 지정과 용량 제한, 이름 지정을 수행해주는 일종의 방법이다. 파티션을 생성하면 메모리 이용을 위해 기존 데이터들이 포맷되고 새로운 파티션이 만들어지는데, 그 과정을 파일시스템을 한다고 말할 수 있다.

파일 시스템의 유형은 리눅스와 윈도우 크게 두 가지로 나누어 볼 수 있다.

리눅스(Linux)	**Ext, XFX, Btrfs, ZFS**
윈도우(Windows)	NTFS, FAT32, UDF, CDFS

여러 파일 시스템들 중, 가장 대표적인 NTFS 파일 시스템과 FAT32 파일 시스템에 대해서 살펴봅시다.

1.2.1 NTFS 파일 시스템

NTFS는 New Technology File System의 의미로, 윈도우 NT의 파일 시스템을 말한다. NTFS는 클러스터 사이즈가 512~4096 바이트 정도밖에 안 될 정도로 작다. 클러스터 크기가 작으면 좋은 점도 있지만, 속도가 느려질 수도 있다는 단점이 있다. NTFS는 FAT32 이후에 나온 파일 시스템이기에, FAT32을 보완하여 더 강력한 기능들을 가지고 있으며, 보안성이 뛰어나다.

1.2.2 FAT32 파일 시스템

FAT은 파일 할당 테이블을 의미한다. FAT32 파일 시스템이 지원하는 드라이브의 최대 크기는 32GB이다. 단일 파일의 최대 크기는 4GB이며, 해당 크기 초과시 복사가 불가능하다. NTFS보다 단순하기 때문에 작은 볼륨에서는 액세스 속도가 더 빠르다. 그리고 파일 이름 지정 시 길이에 제한이 있다는 특징이 있다. 하지만 구형 운영체제, 리눅스, iOS 등 거의 모든 디바이스와 호환된다는 장점이 있다. NTFS와 비교해서는 안정성과 보안성이 다소 낮다.

2. 파티션의 손상

파티션이 손상되는 경우에 대해 알아보고자 한다. 하드디스크 파티션이 손상되는 원인은 파티션 삭제, 디스크의 물리적인 손상, OS 스토리지 관리자 오류 등 다양하다. 손상의 해결 방법도 원인에 따라 상이하다.

2.1 PC의 부적절한 종료 또는 정전

파티션 손상되는 원인들 중 가장 일반적으로 많이 발생하는 원인으로 볼 수 있다. 컴퓨터가 부적절하게 종료된다고 파티션 손상이 항상 발생하는 것인 아니지만, 부적절하게 종료될 때 시스템이 돌아가는 중이라면 파티션이 손상될 수 있다. 따라서 주로 타이밍에 기반한다고 볼 수 있다.

2.2 디스크 관리 작업 및 타사 도구 수행 중의 오류

디스크 관리 작업을 수행하는 동안 파티션 크기가 적절하지 않거나 오류가 발생하면 파티션이 손상되고 데이터가 유실될 수 있다. 타사의 디스크 관리 도구도 잘못 사용시 드라이브의 구조를 변형하여 파티션의 손상을 유발할 수 있다.

2.3 불량 섹터

2.1의 원인과 더불어 일반적으로 발생할 수 있는 원인이다. 불량 섹터는 일반적으로 논리적 오류 또는 디스크의 물리적 손상으로 인해 발생한다. 이유가 어떻든 불량 섹터는 일반적으로 파

티션 손상 및 데이터 손실을 유발한다.

2.4 파티션 테이블의 손상

파티션 테이블은 파티션의 모든 세부 정보를 포함하며, 하드 디스크의 첫 번째 섹터에 위치한다. 이 테이블이 손상되면 전체 드라이브를 읽을 수 없게 되고 파티션이 손상된다.

3. 파티션 복구 방법

3.1 cmd 명령 프롬프트 창을 사용하는 방법

A. 윈도우키와 R키를 동시에 누른 뒤, 실행상자가 뜨면 "cmd"를 입력하고 관리자 권한으로 명령 프롬프트를 실행시킨다.

B. Diskpart창 옆에 입력을 한 뒤 엔터를 친다.

C. 유형 목록 디스크와 엔터를 친다.

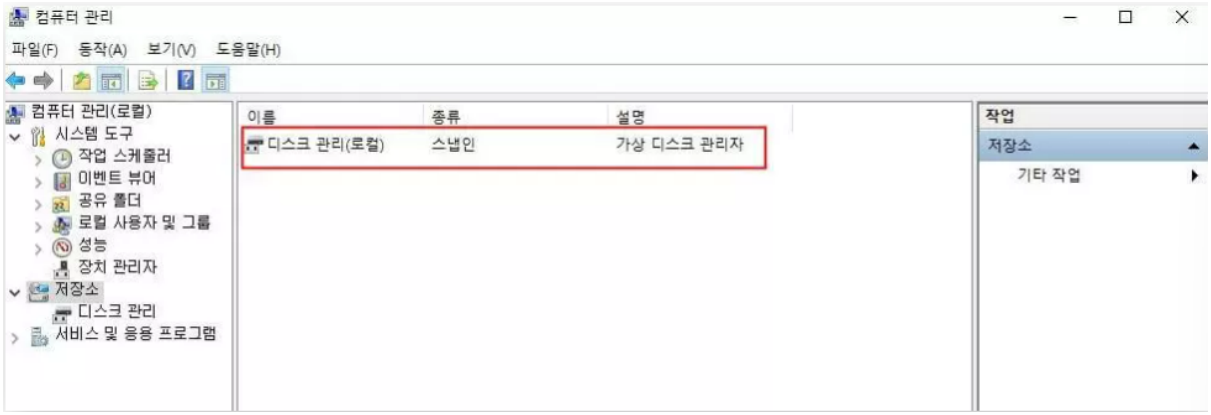
D. 컴퓨터의 모든 디스크가 표시되면 디스크 번호를 입력한 뒤 엔터를 친다.

E. 유형 목록에 볼륨#을 한뒤, 유형목록에 할당하고 편지=#키를 클릭한다.

F. 프롬프트 종료 후 파티션이 되살아났는지 확인한다.

3.2 파일 시스템을 사용한 파티션 포맷 및 파티션 생성

파티션 같은 경우, 실수로 포맷되거나 손상되는 경우도 있지만, 디스크 공간의 효율적 활용을 위하여 일부러 포맷을 진행하는 경우도 있다. 이에 대하여, 데이터를 복구한 후 디스크 파티션을 생성하고, 포맷하는 방법을 소개하고자 한다.



A. 시작 단추를 클릭하고, 컴퓨터 관리를 실행한다 -> 제어판-시스템 및 보안-관리도구를 탭한 뒤 컴퓨터 관리를 두 번 클릭

B. 좌측 저장소 칸에 있는 디스크 관리를 탭한다.

C. 하드 디스크에서 할당되어 있지 않은 영역을 마우스 우클릭 한 뒤 새 단순 볼륨은 탭한다.

D. 단순 볼륨 만들기 마법사에서 다음버튼을 누른다.

E. 볼륨 크기를 입력하고(MB단위) 최대 기본 크기를 적용시켜 다음으로 넘어간다.

F. 기존 문자를 적용할 수도 있고 다른 문제를 입력할 수도 있다. 입력 후 다음을 클릭한다.

G. 지금 포맷을 원하면 다음을 클릭하고, 나중에 포맷하려면 이 볼륨을 포맷하지 않음을 클릭한다.

H. 검토 후 마침을 누른다.

4. 참고자료

- https://dakuo.tistory.com/60
- https://blog.naver.com/jeongsy_-_/222849584084
- https://iboxcomein.com/file-system-ntfs-fat32-exfat/#ftoc-heading-6
- https://www-dbpia-co-kr.libproxy.sungshin.ac.kr/pdf/pdfView.do?nodeId=NODE02238401
- https://www.remosoftware.com/info/kr/damaged-partition-recovery/#part3

외장 하드 디스크

외장 하드 디스크(External hard drives)는 외장형 케이스에 하드 디스크를 결합한 제품을 일컬어 부른다. 컴퓨터에 연결하면 하드 디스크 형태로 인식하며 다양한 용량의 제품이 시중에 판매 되고 있다. 고용량과 휴대성을 동시에 지니고 있는 저장매체로 주로 백업이나 용량 확장, 하드 카피 등의 용도로 이용한다.

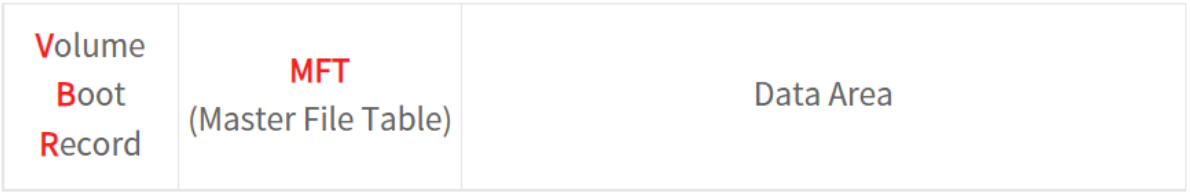
- 장점
  - 저장 용량에 비해 저렴한 가격
  - 안정적인 데이터 보관. 외부 요인을 제외한다면 반영구적으로 데이터를 보관할 수 있다.
  - 파일이 삭제된 경우 USB 나 SSD 에 비해 복구 확률이 높다.
- 단점
  - 외부 충격에 약해 고장이 나기 쉽다. 외장 하드를 휴대용으로 들고 다닐 경우 크고 작은 충격으로 사용 수명이 짧아진다.
  - 크기가 클수록 전력 소모량이 높아져 휴대성이 떨어진다.
  - 분실 위험

외장 하드 디스크의 손상

외장 하드 디스크의 손상은 크게 소프트웨어적(논리적) 손상과 하드웨어적(물리적) 손상으로 구분할 수 있다.

- 소프트웨어적 손상

  소프트웨어적 손상으로는 시스템 오류, 사용자의 비의도적인 데이터 삭제, 포맷과 같이 복구 프로그램을 이용하거나 기타 방법을 통해 복구 처리가 가능한 손상을 일컫는다. 이러한 소프트웨어적인 손상의 공통점은 사용자가 원하는 파일이 삭제되거나 접근할 수 없게 된다는 것이다. 이는 Windows가 사용하는 파일 시스템과 관련이 있는데 그 중 대표적인 NTFS 파일 시스템을 예로 들 수 있다. NTFS에서 파일이 디스크에 저장되는 방식은 다음과 같다.



  왼쪽에서 두 번째 영역인 MFT는 파일에 관한 정보가 기록되고, 실제 파일의 데이터는 Data Area에 기록 된다. 즉, 실제 파일의 내용은 Data Area에, 해당 파일의 이름과 속성, 기록된 위치 등과 같은 파일의 메타 데이터는 MFT에 기록되는 것이다. 이러한 방식으로 파일을 관리한다면 사용자가 원하는 파일에 접근하기 위해 MFT를 우선 탐색하고 곧장 해당 파일의 위치를 확인할 수 있어 효율적인 파일 탐색이 가능해진다.

  이런 파일 시스템의 구조로 인해 MFT의 정보에 오류가 발생하게 되면 데이터를 찾지 못하는 상황으로 이어진다. 실제로 데이터는 삭제한다는 것은 Data Area에 있는 데이터 내용을 지우는 것이 아니라 MFT에 있는 해당 파일이 저장된 위치 정보를 지워 파일이 존재하지 않는 것처럼 인식시키는 것이기 때문이다. 일반적으로 사용하는 디스크 복구 프로그램은 이러한 원리를 이용해 Data Area에서 직접 파일을 찾아 MFT에 파일이 위치한 실제 주소를 다시 기록하고 수정하는 방식으로 파일을 복구하게 된다. 포맷 역시 MFT 영역을 초기화 하는 것이기 때문에 데이터 복구가 가능한 것이다.

  - 소프트웨어적 손상을 유발하는 다양한 원인
    - Windows 시스템의 충돌로 인한 오류
    - 사용자 PC 가 MFT 를 공격하는 멀웨어 및 바이러스에 감염 된 경우
    - 하드 드라이브의 불량 섹터 다량 존재
    - 애플리케이션 간의 충돌 혹은 오작동
    - 외부 디스크에 저장된 데이터 접근, 이용 중 갑작스러운 연결 분리

- 하드웨어적 손상

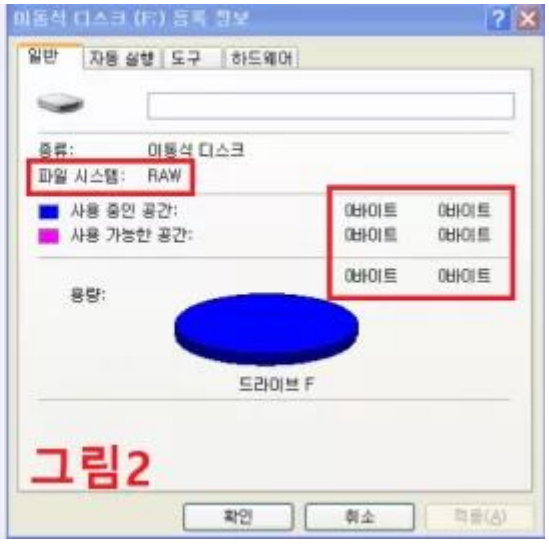
  하드웨어적 손상은 파일 시스템이나 데이터 문제가 아닌 외장 하드 디스크 장치 발생한 물리적 손상이다.

  - 하드웨어적 손상을 유발하는 다양한 원인
    - ○ 컴퓨터 혹은 외장 하드 디스크에 물리적인 충격이 가해진 경우
    - ○ 접속 도중 강제 종료
    - ○ 침수
    - ○ 컴퓨터와 외장 하드 디스크 케이블의 무리한 분리

외장 하드 디스크의 오류 해결 (데이터 복구)

1. 손상 종류 파악하기

   오류가 발생한 외장 하드의 등록정보가 그림 1처럼 나온다면 소프트웨어적 손상이다. 이 경우 파일 시스템과 저장공간이 모두 표기 된다. 반면 그림2처럼 파일 시스템이 RAW로 표시되고 바이트가 1으로 나온다면 물리적 손상일 가능성이 높다.



   혹은 HEX Editor를 이용해 외장 하드 디스크의 HEXA CODE를 확인해 오류의 종류를 파악할 수 있다. Hexa Code가 정상적으로 출력될 경우 소프트웨어적 손상으로, 비정상적으로 출력될 경우 하드웨어적 손상으로 구분할 수 있다.

<복구 관련 추후 추가 실습 시 참고 자료>

https://4ddig.tenorshare.com/kr/hard-drive/fix-logical-and-physical-faults-of-external-hard-drive.html