01 파일 복구 이해

1 파일 복구

▪ 파일 복구

- Data Recovery

- 손상, 접근 불가, 은닉, 잔존되어 있는 Data를 분석할 수 있도록 복구하는 기술

- Data Recovery를 위해 요구되는 기술

- File System의 이해
- OS와 File System간의 메커니즘 이해
- 응용 프로그램과 관련된 파일 구성의 이해
- 응용 프로그램과 관련 파일간의 메커니즘 이해
- 다양한 복구 기법과 원리의 이해
- 관련 도구(Encase, FTK, …)들의 이해

01 파일 복구 이해

1 파일 복구

▪ Logical Data 저장 위치와 특성

- **Regular files**

- 사용자 관점에서 Data가 정상적으로 저장되어 있는 파일

- Filesystem의 metadata(MAC Time, File Name 등), 파일 내의 metadata를 이용하여 추가 정보 획득 가능

- **Temporary files**

- 임시 파일로서 경우에 따라 삭제되는 경우 발생

- 암호화된 관련 파일의 평문 저장 가능

- **Deleted files**

- 사용자에 의해 삭제된 파일로서 overwritten되지 않으며 간단히 복구 가능

- **Retained Data Block**

- 파일이 삭제되어 논리적으로 존재하지 않지만 일부 또는 전체 Data가 잔존하는 Block

- Slack space 또는 할당되지 않은 Disk 영역에 잔존하며 overwritten 될 수 있음

01 파일 복구 이해

1 파일 복구

▪ Logical Data 저장 위치와 특성

- **Hidden blocks**

- Vender에 의해 별도로 할당된 블록(복구용)으로서 HPA(Host Protected Area) 등이 있음
- OneNAND와 같은 Flashmemory에서 OTP(One Time Programmable)와 같은 영역

- **Bad blocks**

- 저장장치의 이상으로 일부 blocks이 bad로 설정된 block
- 실제 정상적인 block이나 임의로 bad로 설정된 경우도 존재

- **Backup data**

- 동일한 저장장치 또는 별도의 분리된 장치에 저장된 data

- **Unused space**

- 저장된 정상 데이터의 size가 변경되지 않아 일정한 Slack space를 보장 받을 수 있는 공간
- 임의로 File 또는 Filesystem Spec.의 유연성을 이용하여 space를 확보하고 Data 저장

01 파일 복구 이해

1 파일 복구

▪ Data Recovery 분류

- **Physical Recovery**

- 손상된 PCB 등 부품 교체
- MFM(Magnetic Force Microscopy) 장비를 이용한 Scanning

- Logical Recovery

- Partition Recovery
- Undeletion
- Signature Search
- Data Carving
- Finding hidden data
- Password recovery, Decryption
- Steganalysis
- Unpacking, decoding
- Reverse Engineering
- Etc…

01 파일 복구 이해

1 파일 복구

▪ Data Recovery 분류

- **Partition Recovery**

- MBR의 Partition Table에 잔존하는 정보를 이용한 Partition 복구
- Partition Table 없이 File System Signature를 이용한 복구

- **Undeletion**

- 삭제된 파일은 실제 파일 Data가 삭제되지 않고 파일 Index의 일부 정보만 삭제
- 이러한 남겨진 Index 정보를 이용하여 복구

- **Signature Search**

- Application이 자신과 관련된 File을 Load할 때 정합성을 검사하기 위해서 일정한 값(표식)을 File의 처음 또는 끝 부분에 표시하고 있음
- 이러한 표식 값을 검사하여 파일을 복구

- **Data Carving**

- File System 정보 없이 순수 Low Image에서 파일을 검색하고 복구하는 기법

01 파일 복구 이해

1 파일 복구

▪ Data Recovery 분류

- **Finding hidden data**

- Disk에서 사용하지 않는 영역, 의도적으로 사용되지 않는 영역으로의 조작 등으로 발생한 영역에 File 또는 Data를 은닉했을 때 이를 복구

- **Password recovery, Decryption**

- 파일이 존재하지만 암호화되어 있어 일반적으로 복구할 수 없는 경우
- 암호화에 사용된 Key를 찾기 위해서 BFA, Dictionary Attack 등을 수행하거나 암호화 알고리즘 또는 암호 프로그램의 취약성을 이용하여 복구

- **Steganalysis**

- Steganography와 같이 파일의 사용되지 않는 영역(not used, reserved), 사용되지 않는 bit 영역, 임의로 사용되지 않는 영역을 삽입하는 방법으로 숨겨진 Data를 복구하는 기법

01 파일 복구 이해

1 파일 복구

▪ Data Recovery 분류

- **Unpacking, decoding**

- Packing: 파일에 저장된 Data가 중복되고 반복되는 데이터가 많아 불필요하게 Size가 큰 파일을 효율적으로 압축하는 기술
- Packing은 일부러 내용을 어렵도록 하여 Data를 직접 분석하는데 시간이 오래 걸림 (관련 프로그램 필요)
- Packing 알고리즘을 이용하여 Unpacking하여 복구하는 기법
- Encoding: 영문자 [SPACE]는 HTTP 상에서 전송될 때 %20 으로 표시하여 전송하며 이러한 변환을 Encoding이라고 함
- Decoding: %20과 같이 일반적인 문자로 해석하기 위하여 [SPACE]로 변환하는데 이러한 과정을 Decoding이라고 함

- **Reverse Engineering**

- Binary로 되어 있는 응용프로그램을 분석하기 위해서 Assembly 언어 또는 C언어와 같이 분석자가 해석할 수 있는 코드로 변환하는 기법

01 파일 복구 이해

② 파일 카빙

▪ 파일 카빙 개요

-Digital Forensic Research Workshop (DFRWS)'s proposal

- "Data caving은 대량의 데이터 집합에서 데이터들을 추출하는 처리를 말한다. 이러한 기술은 파일시스템의 비할당 영역에서 파일을 추출하고자 할 때 사용된다. 각 파일의 특정한 header와 footer 값을 사용해서 비할당 영역에서 파일이 추출되며 이 과정에서 파일시스템 구성 정보를 이용하지 않는다."

2 파일 카빙

▪ 파일 카빙 분류

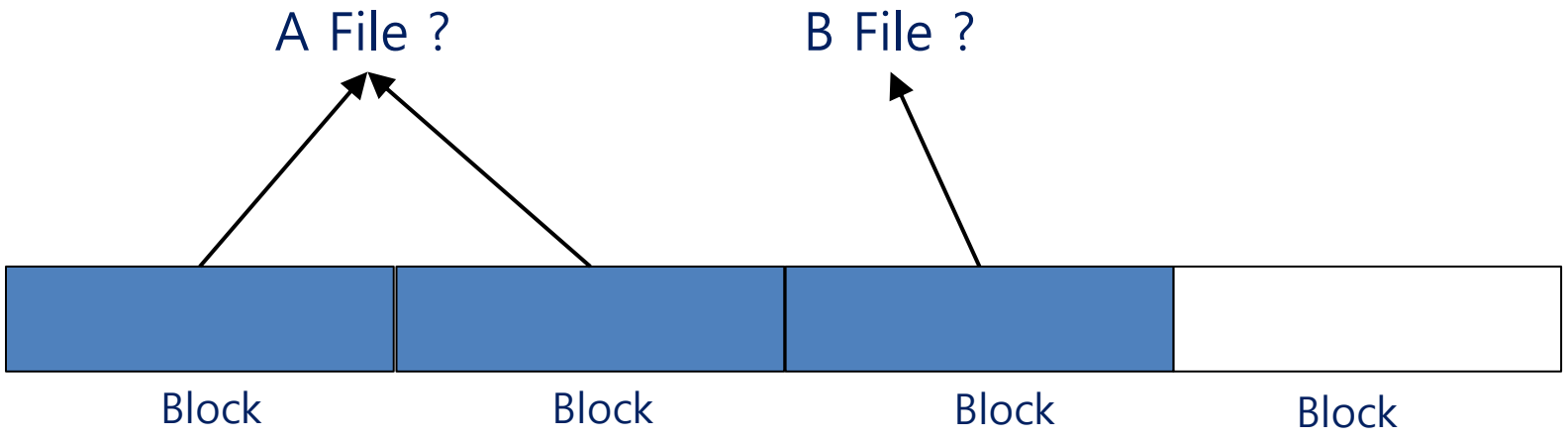
- **Simson Garfinkel and Joachim Metz's proposal**

- Block-based Carving
- Header/Footer Carving
- Header/Maximum (file) size Carving
- Header/Embedded Length Carving
- File structure-based carving 카 빙
- Statistical Carving
- Fragment Recovery Carving
- Repackaging Carving

② 파일 카빙

▪ Block-based Carving

- Block 단위로 분석
- 일반적으로 파일을 저장할 때 Block(Sector)단위로 저장된다는 것을 이용
- 각 Block을 검사하여 파일의 구성 Block 여부를 판별

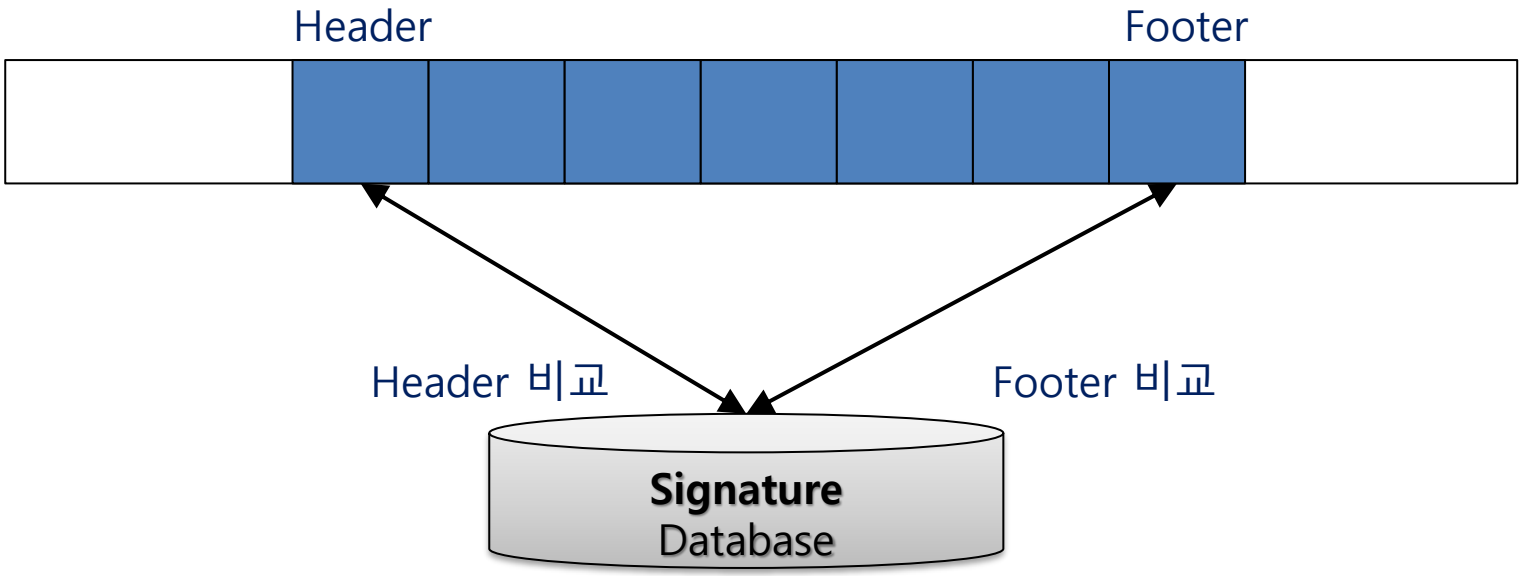


② 파일 카빙

- **Header/Footer Carving**

- 각 File의 Header 또는 Footer의 Signature (or Marker, Magic number)를 이용하여 Carving
- JPEG의 경우 Header/Footer를 가지고 있어 유용

단, 파일 구성이 순차적으로 연속되어 있어야 성공 확률 높음



01 파일 복구 이해

2 파일 카빙

▪ Header/Footer Carving

- 포렌식 분석 기법으로 가장 일반적으로 사용되는 기법
- 파일의 종류를 파악하기 위하여 header 또는 footer의 고유값 (Magic number, signature)를 분석
- 파일의 확장자를 변경했을 경우 탐지 가능

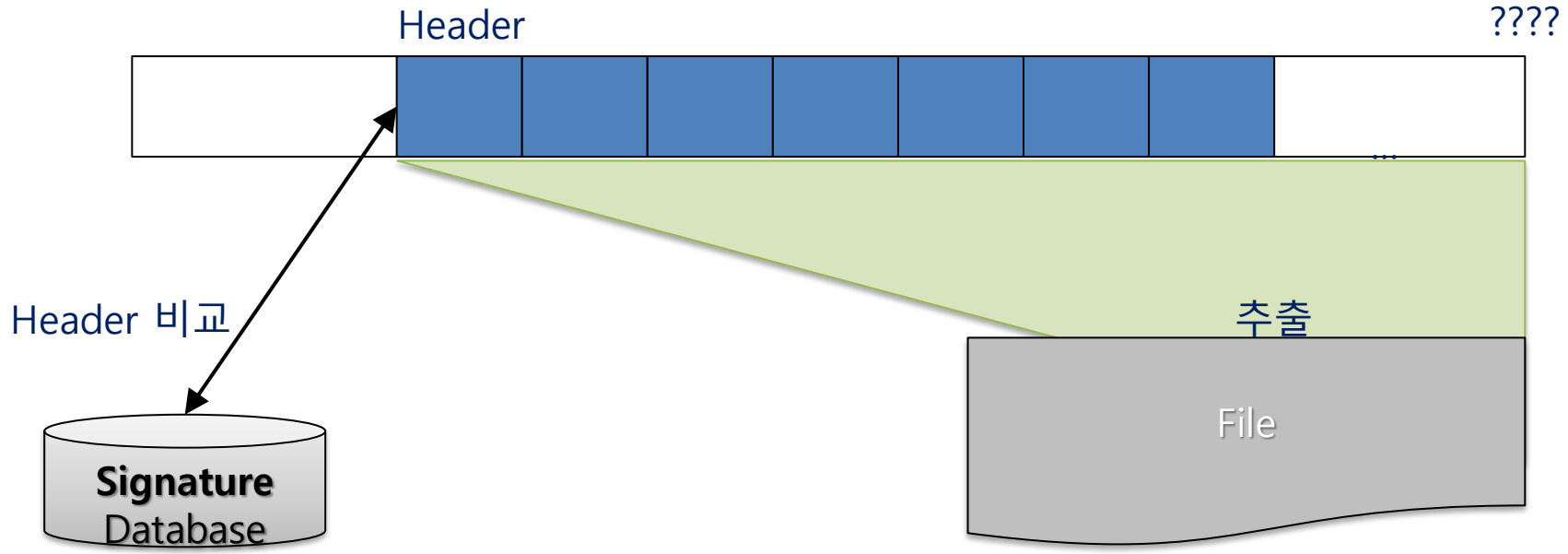
▪ 주요 파일 시그니처 (Signature)

Extention	Signature	Description
PST	21 42 44 4E ! B D N	Microsoft Outlook Files
PDF	25 50 44 46 % P D F	Adobe Portable Document Format File
ISO	43 44 30 30 31 C D 0 0 1	ISO-9660 CD Disc Image
GIF	47 49 46 38 37 61 G I F 8 7 a 47 49 46 38 39 61 G I F 8 9 a	Graphics – Graphics Interchange Format
DOC, HWP, PPT, XLS, …	D0 CF 11 E0 A1 B1 1A E1	MS Compound Document Format

② 파일 카빙

- **Header/Maximum (file) size Carving**

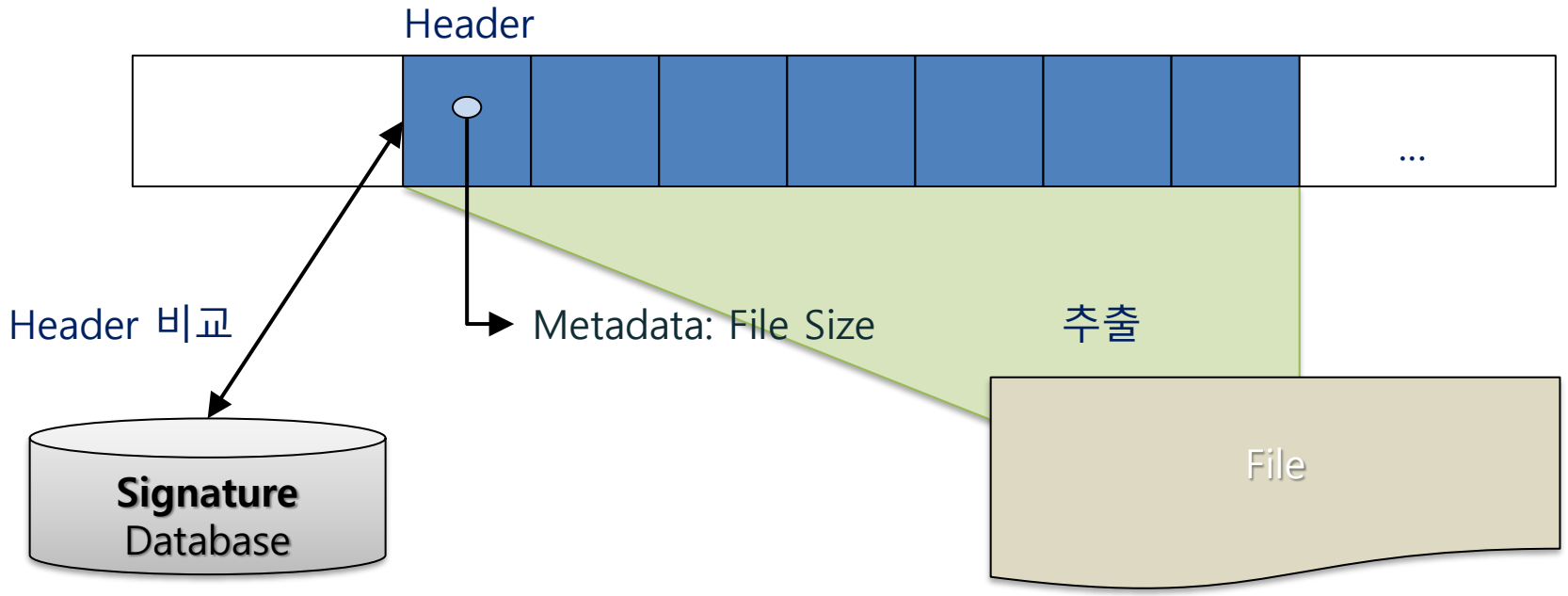
- 각 File의 Singature로 검색 후 Header를 포함하는 섹터부터 최대한 많은 Block을 추출
- 불필요한 데이터가 파일의 끝에 존재해도 정상적으로 Read되는 파일을 추출할 때 유용 (JPEG, MP3 등)



② 파일 카빙

- **Header/Maximum (file) size Carving**

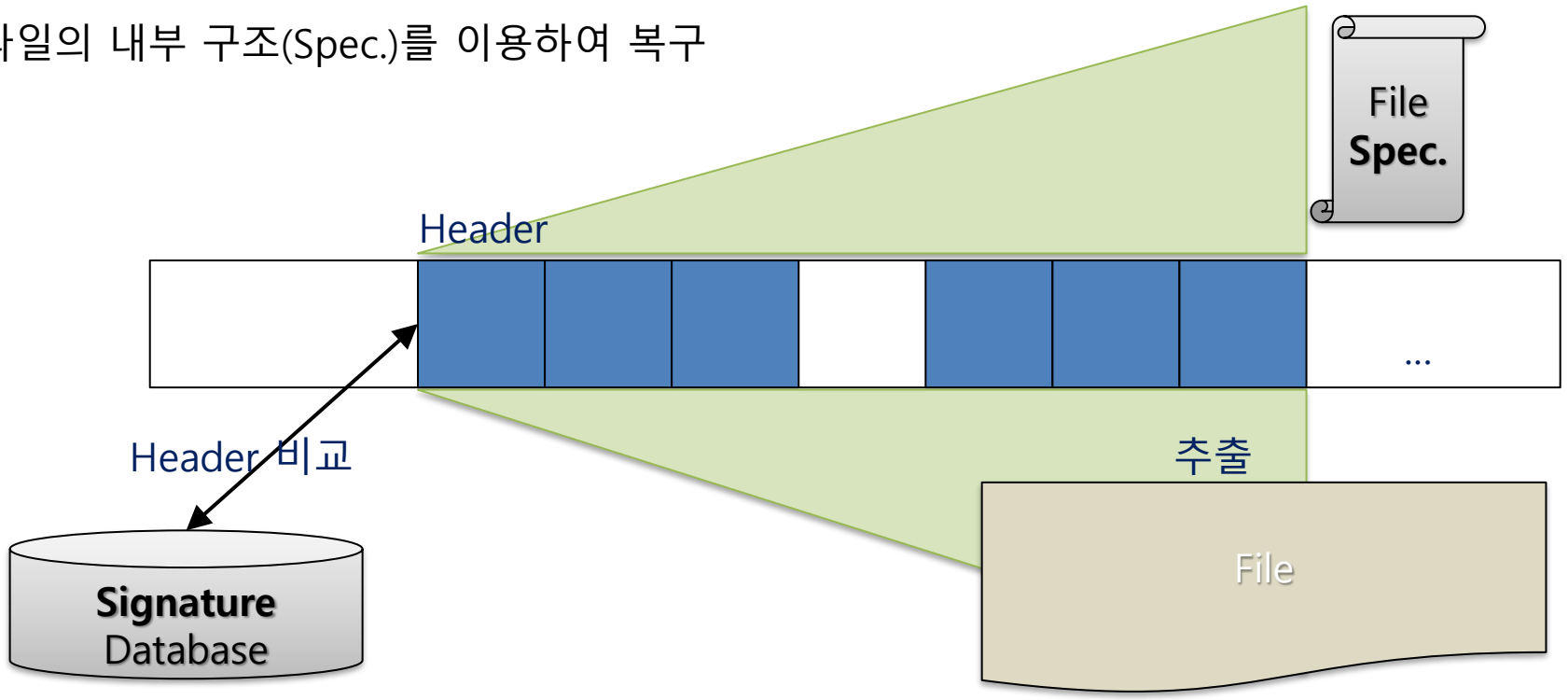
- 각 File의 Singature로 검색 후 파일의 Header 또는 metadata에 포함되어 있는 파일 Size 정보를 이용하여 추출



② 파일 카빙

- **File structure-based Carving**

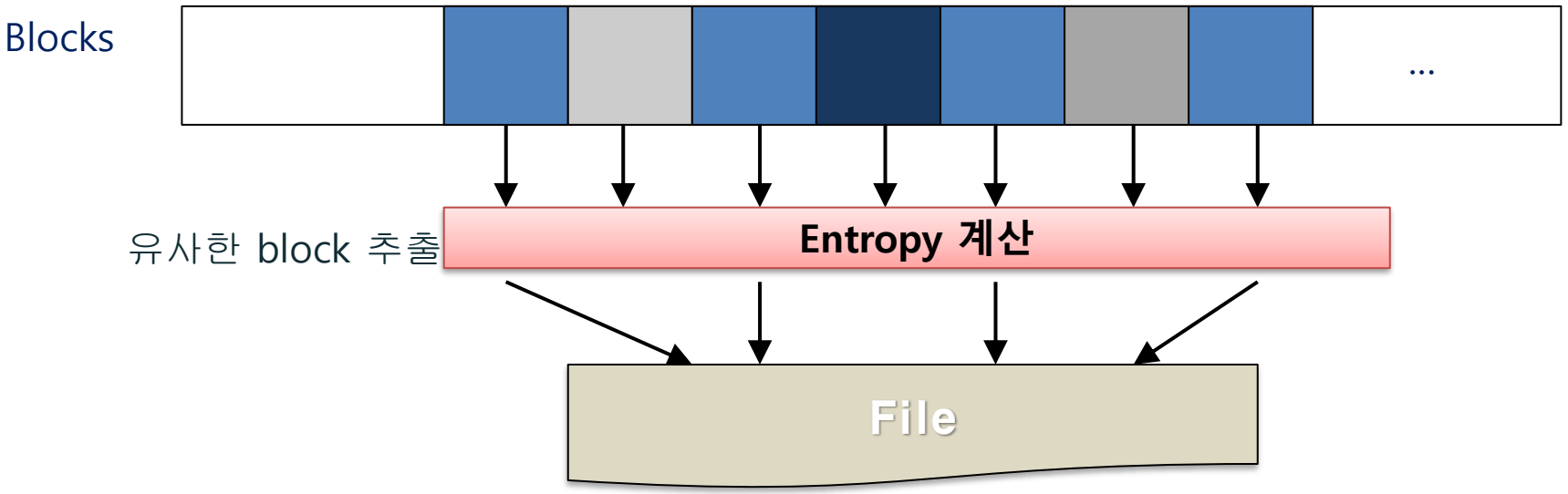
- Semantic Carving (by Garfinkel)
- Deep Carving (by Metz and Mora)
- 파일의 내부 구조(Spec.)를 이용하여 복구



② 파일 카빙

- **Statistical Carving**

- 엔트로피(Entropy, 정보에 포함되어 있는 불확실성의 정도)와 같은 특성이나 통계값을 이용한 복구 기법



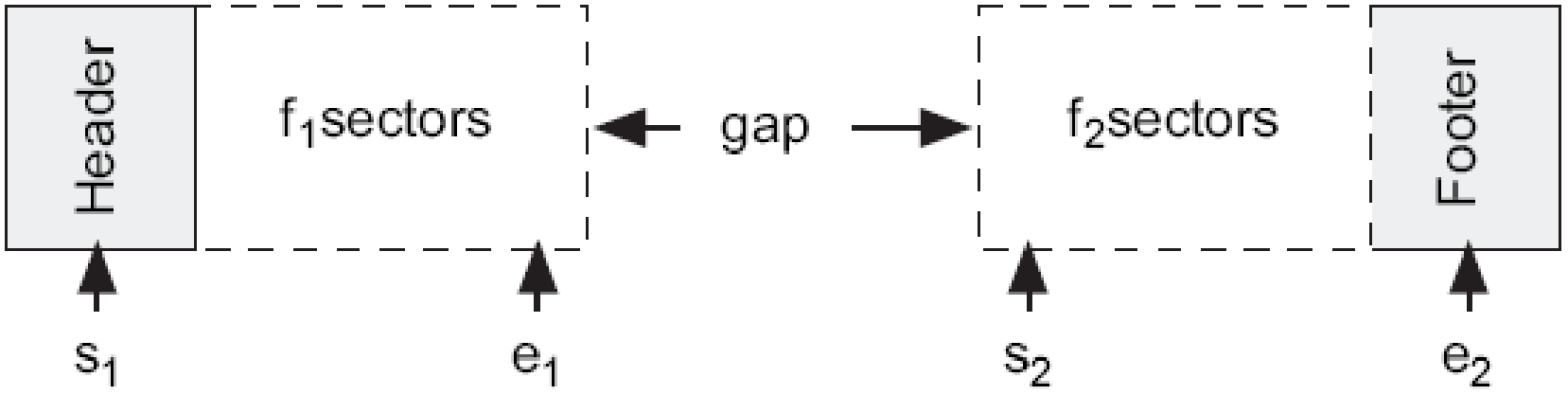
② 파일 카빙

▪ Fragment Recovery Carving

- 단편화된 Block들을 정상적인 파일로 재조립하는 기법
- Split Carving이라고도 함(Garfinkel)

• 관련 Carving 기술

- Bifragment Gap Carving (Garfinkel)



Bifragment Gap Carving

② 파일 카빙

▪ Repackaging Carving

- 추출한 Data에 Header, Footer 또는 다른 정보를 수정 또는 추가하는 기법
- Overwitten, 단편화 등으로 인하여 View가 불가능할 때 인위적으로 수정하여 View 가능하도록 시도하는 기법
- 관련도구: Garfinkel's ZIP Carver