SQL Server Forensic

AhnLab A-FIRST

Rea10ne

unused6@gmail.com

Choi Jinwon

Contents

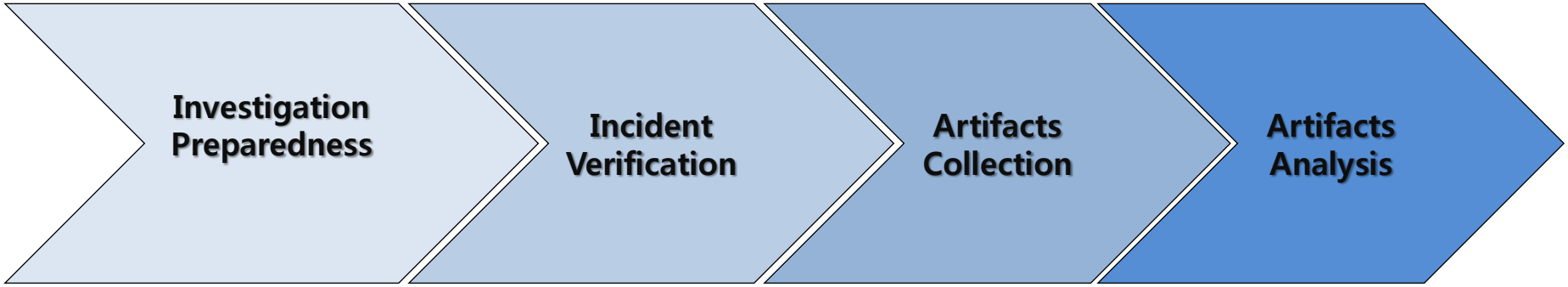
SQL Server Forensic

- What is SQL Server Forensic
- SQL Server Forensic Methodology

What is the SQL Server Forensic

- Database 내에서 발생한 침해사고에 대한 입증 혹은 반증
- Database 침해사고에 대한 영향 분석
- 사용자 DML 혹은 DDL 사용 행위 추적
- Database에서 이전 혹은 이후에 발생하는 Transaction 식별
- 삭제된 데이터 복원

SQL Server Forensic Methodology



- Investigation Preparedness
- Incident Verification
- Artifacts Collection
- Artifacts Analysis

SQL Server Artifacts

- Resident Artifacts
- Non-Resident Artifacts
- SQL Server Artifacts
- SQL Server Artifacts Category

Resident Artifacts

- SQL Server를 관리하는 목적으로, 시스템 설치 시 기본적으로 설정되는 Artifacts
  - 예) SQL Server Error Log, Data Files 등
  - System의 Version에 따라 차이가 발생할 수 있음
  - 휘발성 데이터(Volatility Data)와 비휘발성 데이터(Non-Volatility Data) 모두 존재함

Non-Resident Artifacts

- SQL Server를 운용하기 위한 필수적인 요소는 아니지만, 연관성을 갖고 동작하는 Artifacts
  - 예) System Event Log, Web Server Log 등
  - 대부분의 Non-Resident Artifacts는 비휘발성 데이터로 구성되어 있음

SQL Server Artifacts

SQL Server Artifacts		
Resident Artifacts		**Non-Resident Artifacts**
Volatility	**Non-Volatility**	
Data Cache Plan Cache Cache Clock Hands Active VLFs Server State Ring Buffer	Database SQL Server Error Logs Data Files Authentication Setting Authorization Catalogs Database User Database Objects Server Versioning SQL Server Logs Jobs Triggers Native Encryption CLR Libraries Reusable VLFs …	System Event Logs External Security Controls Web Server Logs

SQL Server Forensic – Kevvie Fowler

SQL Server Artifacts Category

분류	Artifacts
행위 재구성	Data Cache, Plan Cache, Active VLFs, Reusable VLFs, Server State, Database Objects, AutoEXEC Procedures, Cache Hands, Jobs, Triggers, Trace Files, Server Error Logs
데이터 복구	Active VLFs, Reusable VLFs, Table Statistics, Data Files
인증 및 권한	Authentication Settings, SQL Server Logins, Authorization Catalogs, Database User, Trace Files, Server Error Logs
서버 설정 및 버전	Server Configuration, Collation Settings and Data Types, Native Encryption, Server Versioning
연관성 자료	Database, Data Page, End Points, Schema

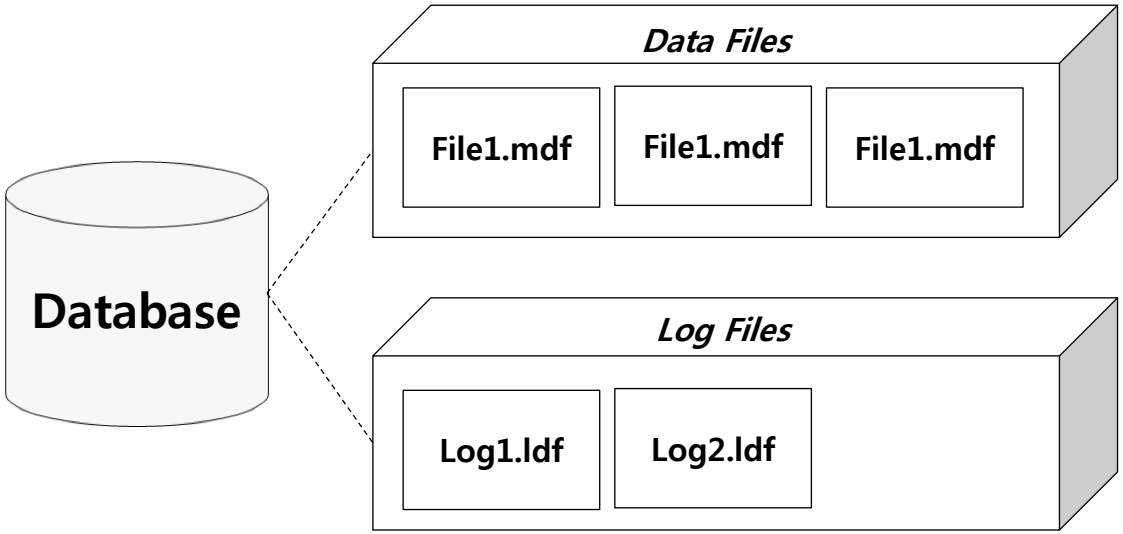
SQL Server Forensic – Kevvie Fowler

Database Files

- Database Files
- Data Storage
- Data Rows & Data Tables
- Data Page
- Extents

Database Files

- 기본적으로 모든 SQL Server는 Data File과 Log이 구성되어 있음
  - Data File : Database Object 들을 저장하고 있는 파일 (*.mdf)
  - Log File : DML(Database Manipulation Language)과 몇몇 DDL(Database Definition Language)의 동작을 기록하는 파일 (*.ldf)
    - ✓ Database의 로그는 이벤트 단위의 로그가 아닌 Transaction 단위의 로그로 기록됨 (Transaction Log)



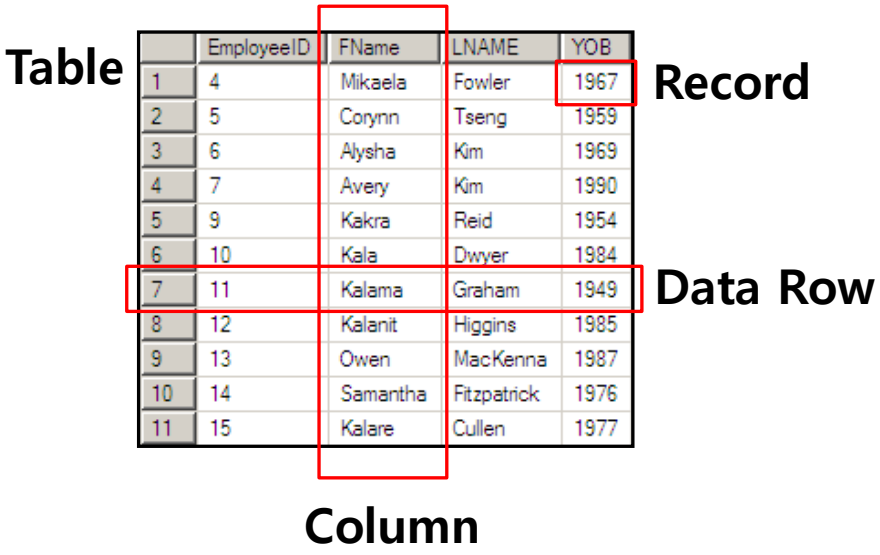
SQL Server Forensic – Kevvie Fowler

Data Storage

- SQL Server는 많은 양의 데이터를 관리하기 위해서 여러 단위의 논리적인 구조를 사용함
  - Records
  - Columns
  - Rows
  - Tables
  - Pages
  - Extents

Data Rows & Data Tables

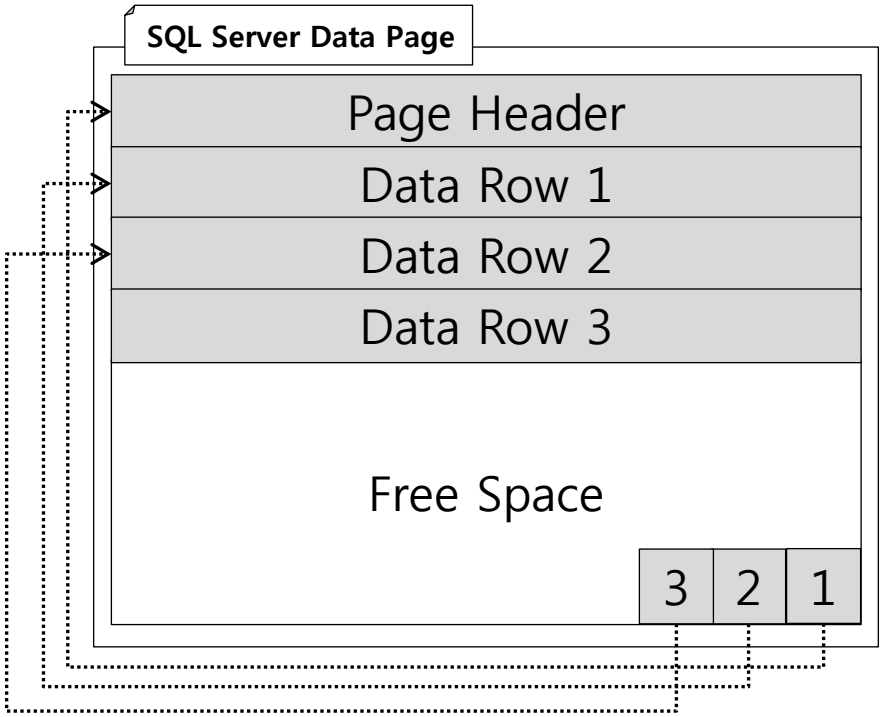
- Data Rows
  - 각 Column에 속해 있는 Record들의 집합으로 이루어진 간단한 구조체
    - ✓ Data Row는 고정적인 사이즈의 데이터를 포함하고 있는 Fixed Rows와 가변적인 사이즈의 데이터를 포함하고 있는 Variable Rows로 나누어 짐
- Data Tables
  - 동일한 Column으로 구성된 Row 들의 집합으로 이루어진 간단한 구조체



	EmployeeID	FName	LNAME	YOB
1	4	Mikaela	Fowler	1967
2	5	Corynn	Tseng	1959
3	6	Alysha	Kim	1969
4	7	Avery	Kim	1990
5	9	Kakra	Reid	1954
6	10	Kala	Dwyer	1984
7	11	Kalama	Graham	1949
8	12	Kalanit	Higgins	1985
9	13	Owen	MacKenna	1987
10	14	Samantha	Fitzpatrick	1976
11	15	Kalare	Cullen	1977

Data Page

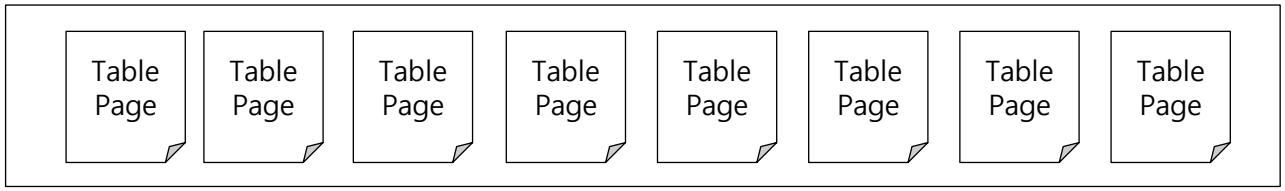
- Data Pages
  - Data Row의 집합으로 되어진 8192 Byte 크기의 구조체
  - Page Header, Data Rows, Rows Offset Array로 구성되어 있음
  - 각 Page들은 Page ID(PID)로 구분되어 짐



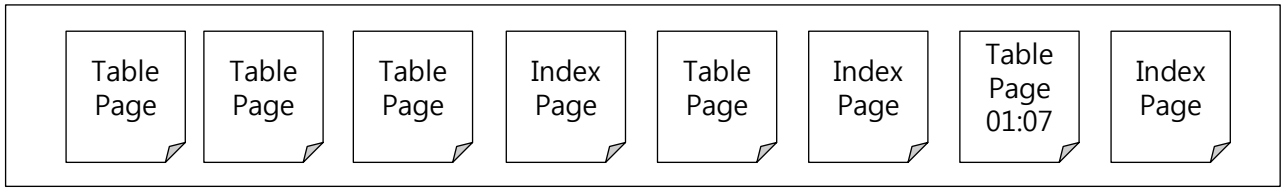
http://msdn.microsoft.com

Extents

- Extent
  - 8개의 연속된 Page로 구성된 64KB 크기의 구조체
  - Extent를 구성하는 Table과 Index에 따라 Uniform Extent, Mixed Extent로 구분됨
    - ✓ Uniform Extent : 동일한 종류의 Page로 구성된 Extent



    - ✓ Mixed Extent : 서로 다른 종류의 Page로 구성된 Extent



Recovering Deleted Data From Data Files

- Data Recovery
- Identifying Data Rows Offset
- Extract the Delete Data Row
- Data Row Reconstruction

Data Recovery

- SQL Server Data Recovery
  - Identifying Deleted Data
  - Data Geometry
  - Data Writing mechanism
  - Overwriting (First Available or Next Available)
  - Data Row Internal Structure

Identifying Deleted Data Rows

- 조사하고자 하는 Table이 포함되어 있는 Data Page를 식별함
  - MS-SQL의 DBCC(Database Console Command)를 통해 식별하도록 함
  - 조사하려는 Table의 PageFID와 PagePID를 확인함

```
DBCC TRACEON (3604)
DBCC IND (DB_Name, Table_Name , -1 ) -- 해당 테이블에 할당된 모든 PageID를 출력

DBCC TRACEON (3604)
DBCC IND (DB_Name, Table_Name , 0 ) -- 해당 테이블의 내용이 포함된 PageID를 출력
```

  - 확인된 ID들을 통해 해당 Page의 내용을 확인함

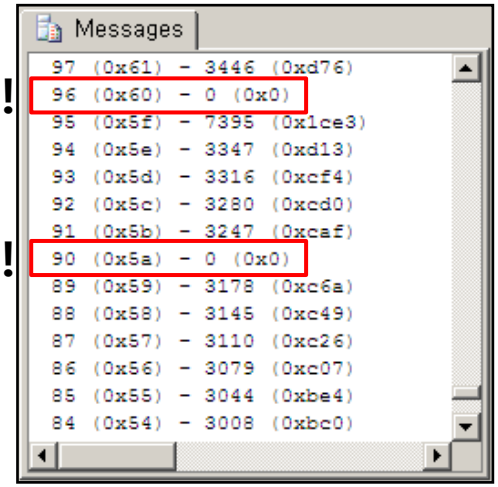
```
DBCC TRACEON (3604)
DBCC PAGE (DB_Name, File_ID, Data_Page, 1) -- 각 Row의 메타데이터를 포함하여 출력

DBCC TRACEON (3604)
DBCC PAGE (DB_Name, File_ID, Data_Page, 2) -- Page File의 내용을 Raw Data로 출력
```

Extract the Delete Data Row

- Data Rows Offset Array에서 삭제된 데이터의 ID와 Offset 정보를 확인할 수 있음
  - 삭제된 데이터는 Data Rows Offset Array 필드의 값이 0x00으로 변경됨

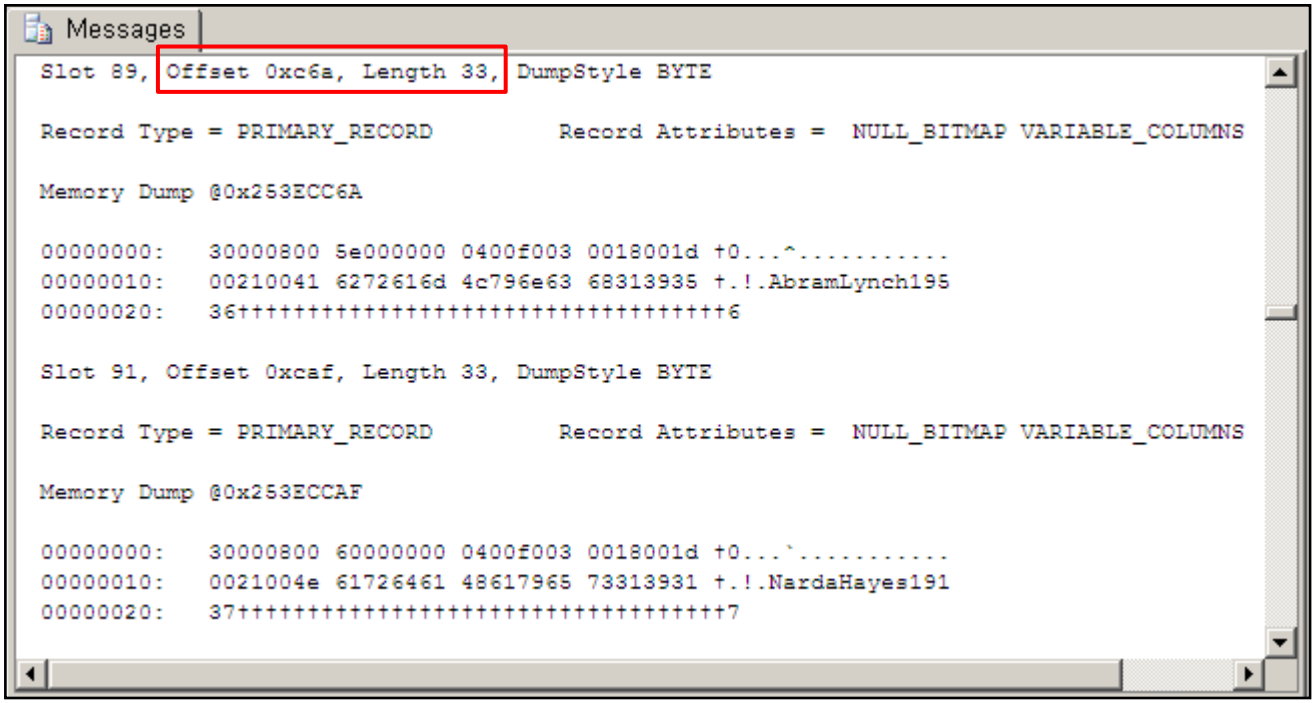
Deleted Rows!!

Deleted Rows!!



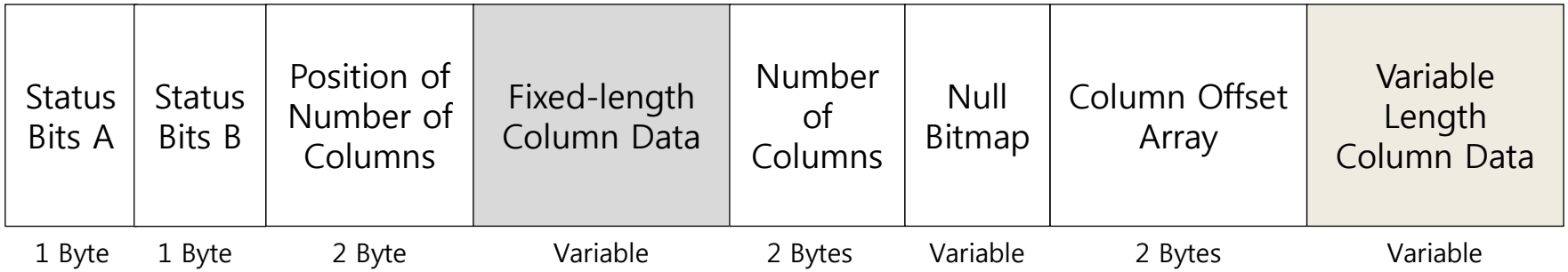
  - Offset Array에서 0x00으로 변경된 Rows의 Offset 정보를 확인함
    - ✓ Offset Array에는 삭제된 Row의 Offset 정보는 초기화 됨
    - ✓ 삭제된 Row 앞에 존재하는 Row의 Offset과 Size 정보를 통해 삭제된 Row의 Offset 정보를 확인함

- Offset Array에서 0x00으로 변경된 Rows의 Offset 정보를 확인함
  - Offset Array에는 삭제된 Row의 Offset 정보는 초기화 됨
  - 삭제된 Row 앞에 존재하는 Row의 Offset과 Size 정보를 통해 삭제된 Row의 Offset 정보를 확인함



Data Row Reconstruction

- Data Row Structure



Component	Description
Status Bits A	Data row 속성을 표현하는 status bit A
Status Bits B	SQL 2000, 2005, 2008에서는 사용하지 않음
Position of Number of Columns	Number of Columns의 Offset
Fixed-length Column Data	고정 길이 데이터 필드
Number of Columns	해당 Data Row에 있는 Column 들의 전체 개수
Null Bitmap	Column Data의 사용 현황
Column Offset Array	각 가변 길이 데이터의 Offset 정보 (끝 지점을 나타냄)
Variable Length Column Data	가변 길이 데이터 필드

Question and Answer